+ EN CADEAU : **2 magazines complets offerts** SUR LE CD

LES CAHIERS DU HACKER

PIRATE [INFORMATIQUE] // 24

0% PUB 0% CENSURE

GUIDE PRATIQUE!
avec CD GRATUIT
> Les meilleurs logiciels avec PAS À PAS !

BEST OF 2015

PIRATAGE

Tous les outils
Tous les tutoriels

- Anonymat
- Cracks
- Sous-titres
- Applications
- Mots de passe
- Mediacenter
- Raspberry Pi
- Prise de contrôle

ENQUÊTE SPÉCIAL DARKNETS

Les réseaux secrets du WEB INTERDIT

HACKING

Hacker sa voiture : un jeu d'enfant



TÉLÉCHARGEMENT

Le guide pratique du téléchargement direct



PROTECTION

Kali Linux : Un PC qui auto-détruit ses données

SOMMAIRE

PROTECTION/ANONYMAT

HACKING

MULTIMÉDIA



38



LES CAHIERS DU HACKER
PIRATE [INFORMATIQUE]

N°24– Jan. / Mars 2015

Une publication du groupe ID Presse.
27, bd Charles Moretti - 13014 Marseille
E-mail : redaction@idpresse.com

Directeur de la publication :
David Côme
Locke Cole : Benoît BAILLEUL
Gau : Yann Peyrot
Sabin & Edgar Figaro :
Stéphanie Compain & Sergueï Afanasiuk
Terra Branford : Karima Allali

Imprimé en France par / Printed in France by :
Léonce Deprez
ZI Le Moulin 62620 Ruitz

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 1969 - 8631

«Pirate Informatique» est édité par SARL ID Presse, RCS : Marseille 491 497 665
Capital social : 2000,00 €
Parution : 4 numéros par an.

ÉDITO

L'actualité a été chargée sur la fin de cette année 2014. Nous avons eu le droit à l'histoire de la Corée du Nord qui pirate Sony pour protester contre la sortie d'un film se moquant de leur *«Dirigeant bien aimé»* (franchement vous y croyez vous?) ainsi qu'à la blague du piratage des serveurs de Sony (encore ?) et Microsoft par la Lizard Squad juste au moment où des milliers de consoles sont au pied du sapin. Nous avons eu aussi le droit à l'analyse des documents dévoilés par Snowden permettant de déterminer que certains outils comme le chiffrement AES, le protocole HTTPS ou les VPN ne sont plus sûrs pour garantir notre vie privée. Et que dire du revirement tactique des djihadistes de l'EI qui se sont rendu compte (comme leur camarade de jeu américain peu avant) que les réseaux sociaux sont parfaits pour la propagande, mais beaucoup moins lorsque des troufions partagent sur leurs murs des endroits censés être secrets. Espérons que 2015 soit aussi prolifique en actualités désopilantes !

Comme à chaque fois, vous retrouverez sur notre CD tous les logiciels dont nous parlons dans le magazine ainsi que certains anciens articles qui vous aideront à mieux comprendre nos démonstrations. Enfin, nous vous invitons à vous rendre page 37 pour vous abonner gratuitement à la mailing-list de magazine et être tenu au courant des parutions.

N'hésitez pas à nous faire part de vos commentaires et de vos souhaits pour les prochaines éditions sur **benbailleul@idpresse.com**

Bonne lecture !

Benoît BAILLEUL.

HACKTUALITÉS

GOOGLE BALANCE SES UTILISATEURS



Voici une petite histoire passée inaperçue en France, mais relayée par notre confrère Korben.info... La chaîne YouTube Al-Hayat, qui diffuse des actualités en rapport avec le monde arabe et qui critique l'intégrisme islamique a reçu des plaintes de la part de Google. La firme a reçu par formulaire une demande de la société FirstCrist Copyright prétendant que certaines des images utilisées par Al-Hayat lui appartenaient. Avec sa chaîne suspendue, le seul moyen qu'avait le responsable d'Al-Hayat pour continuer son activité était de dévoiler ses coordonnées en vue de trouver un arrangement avec son accusateur. Le problème c'est que la société FirstCrist n'en était pas une et que derrière ce nom se cachait des barbus pas très familiers avec le concept de liberté d'expression. Google a donc donné à n'importe qui les coordonnées d'un de ses utilisateurs. On peut donc mettre en danger des tiers et les sacrifier sur l'autel du copyright...

WHATSAPP SE MET AU CHIFFREMENT DE BOUT EN BOUT !



Dans notre numéro 22 nous vous avions parlé de TextSecure une application permettant de chiffrer vos messages écrits sur mobiles. Cette appli très performante remplace avec brio l'appli SMS de base, mais son utilisation restait confidentielle puisqu'il faut bien entendu que les différents correspondants la possèdent. C'est donc avec joie que nous vous annonçons que le code de TextSecure a été implémenté de base à toutes les versions de WhatsApp (15 millions de téléchargements rien que sur la plate-forme Android). WhatsApp devient donc le premier service de messagerie grand public à intégrer du chiffrement de bout en bout...

VERACRYPT 100 % COMPATIBLE AVEC LES CONTENEURS TRUECRYPT

Si vous nous lisez régulièrement vous savez que TrueCrypt a cessé son développement l'année dernière. Les rumeurs allaient bon train (menace de la NSA, hack du site ou du code source, etc.), mais toute la communauté était d'accord pour dire que le logiciel était dorénavant peu sûr. Nous avons donc eu le nez creux en vous proposant l'alternative VeraCrypt dans notre *Guide de Pirate numéro 1* puisque depuis cette semaine les conteneurs TrueCrypt sont compatibles avec la dernière version du logiciel ! Plus d'hésitation : VeraCrypt devient donc pour nous la référence en matière de chiffrement de données à la volée. Nous vous proposerons bientôt un article plus détaillé sur ce programme.





SMBC by Zach Weiner

UNE CHARTE ANTI-PUB POUR LUTTER CONTRE DDL

C'est bien connu, les publicitaires ne prennent pas de gants lorsqu'il s'agit de choisir leur support. C'est ainsi que les sites de téléchargement direct regorgent de publicités en tout genre...et pas uniquement de marques marginales. C'est ainsi que le gouvernement a confié à Mireille Imbert-Quaretta (présidente de la Commission de Protection des Droits (CPD) de l'Hadopi) la mission de trouver une solution pour assécher les finances des sites



proposant du contenu illégal. La première mesure consiste à s'entendre avec Google pour que le référencement de ces sites soit moins efficace tandis que la seconde se concentre sur les revenus publicitaires. Le ministère de la Culture vient donc d'annoncer l'élaboration d'une charte d'engagement des professionnels de la publicité contre les sites illicites pour responsabiliser les annonceurs. Prévue pour février 2015, cette charte marque sans doute la fin des publicités Panzani ou Meetic sur film-à-gogo.com. Et pour les autres annonceurs un peu plus «confidentiels» ?

DDOS À LA CARTE !

Les pirates de la Lizard Squad qui se sont dernièrement fait un nom en mettant hors service les réseaux du Xbox Live et du PlayStation Network continuent de narguer les autorités en mettant en ligne leur «Lizard Stresser». Il s'agit en fait d'un service permettant à n'importe qui d'emprunter la force de frappe des bots ayant mis sur la touche les serveurs de Sony et de Microsoft. Pour des prix allant de 5 à 110 € vous



pourrez donc demander à ce qu'un site croule sous les requêtes en vue de le faire planter (attaque DDoS ou Distributed Denial of Service). Bien sûr le groupe de hacker précise que le site a pour but de tester les serveurs des demandeurs, mais à la rédaction nous n'y croyons pas trop. Les récentes arrestations qu'ont connu les membres de la Lizard Squad n'ont pas eu l'air de les traumatiser tant que ça...

Lien : **https://lizardstresser.su**

CE QUE LES DOCUMENTS DE SNOWDEN NOUS APPRENNENT...

Lors d'une récente conférence du CCC (le Chaos Computer Club, une organisation historique de hackers), Jacob Appelbaum et Laura Poitras ont conjointement présenté un tour d'horizon des outils résistants à la NSA ainsi que ceux qui, malheureusement, sont moins efficaces (ou plus du tout). Ces constatations ont été rendues possibles par l'analyse des documents dévoilés par Edward Snowden, le fameux lanceur d'alerte qui passe des vacances forcées en Russie. Et le moins qu'on puisse dire, même si ces éléments datent de 2012, c'est que les résultats sont surprenants. On y apprend notamment que les conteneurs TrueCrypt ainsi que les protocoles PGP et Off-the-Record Messaging sont considérés comme «sûrs». À noter toutefois que TrueCrypt n'est plus considéré comme hermétique après sa version 7.1a par la communauté depuis l'arrêt du développement (voir notre édito du numéro 22).



Tor est toujours d'attaque

La NSA n'est pas non plus à l'aise avec Tor même s'il est toujours possible de placer un nœud-espion ou de sniffer un nœud de sortie dans certaines circonstances. Mais la surprise vient des VPN et des protocoles HTTPS et SSH qui semblent presque transparents pour les services secrets américains : Facebook, Gmail et consorts font donc partie du côté immergé de l'iceberg. Le flou règne en ce qui concerne le chiffrement AES, mais on sait que la NSA met du cœur à l'ouvrage pour le cracker. Attention, même si la NSA arrive à scanner un nombre très important de données, elle n'est pas en mesure de tout «cracker» ou déchiffrer. Par contre, si vous commencez à les intéresser... En partant de ces constatations, les prochains numéros de *Pirate Informatique* mettront l'accent sur les méthodes qui mettent mal à l'aise la NSA pour mettre de côté celles qui deviennent obsolètes...

HACKTUALITÉS

COMMOTION, UN AUTRE INTERNET

Depuis le musellement du Net se pose le problème du contrôle d'Internet. Commotion est un projet révolutionnaire permettant la création de réseaux sans fil à haut débit gratuits, sécurisés et protégeant la vie privée des participants...

Imaginez un réseau d'ordinateurs qui fonctionnerait de manière autonome en recevant et émettant des données en haut débit via le Wi-Fi sans qu'il y ait besoin de serveur ou de nœud pour faire circuler l'information. Avec une simple clé USB munie du logiciel, un ordinateur pourrait devenir une partie intégrante de ce réseau, anonyme et chiffré, bien sûr. Il est possible d'imaginer Commotion sur un simple routeur Wi-Fi ou un smartphone. Cerise sur le gâteau, Commotion peut se connecter à Internet puisqu'il suffit qu'un des appareils du réseau le soit pour que tous les autres profitent de l'accès.

DES HACKERS, DES SOCIOLOGUES ET DES JURISTES POUR UN MONDE MEILLEUR ?

Alors que ce type de projet est généralement chapeauté par des hackers soucieux de leur anonymat, Commotion est financé par l'Open Technology Initiative (OTI). Ce dernier constitue la branche «nouvelle technologie» de la New America Foundation (NAF), une organisation consacrée à la recherche de solutions pour l'Amérique du futur. Notez que c'est donc le gouvernement américain qui est à l'origine de ce projet et qu'un des patrons de la NAF n'est autre qu'Eric Schmidt, l'un des patrons de Google. Nous sommes donc bien loin du monde des hackers anti-gouvernementaux se baladant pieds nus et sentant le patchouli à 5 km ! Le projet Commotion est d'ailleurs constitué d'informaticiens, mais aussi de juristes et de sociologues. Le but est de pouvoir installer en peu de temps une sorte de second Internet après une destruction des moyens de communication : catastrophe naturelle ou guerre. On peut aussi imaginer offrir un accès Internet aux zones blanches ou d'utiliser Commotion comme un outil de contournement dans les pays dictatoriaux. Le premier test en 2012 a été de monter un réseau quelque part entre l'Autriche, la Croatie et la Slovénie prouvant qu'il est possible «d'arroser» une zone frontalière sans forcément être présent dans le pays (voir notre schéma).

INTERVIEW DE RYAN GERETY



Ryan Gerety travaille en tant que «field analyst» à la Open Technology Institute. Elle contribue au développement de Commotion en dialoguant avec les pouvoirs publics (mairie, etc.) et les communautés d'utilisateurs. Malgré son emploi du temps chargé, elle a bien voulu répondre à nos questions.

01 Commotion est fonctionnel, mais reste en développement sur différents supports. Quand pensez-vous sortir une version finale du client Linux ? Qu'en est-il de la version Windows et pensez-vous ajouter d'autres marques de routeur dans la liste de compatibilité ?

Les versions Linux et Windows devraient être prêtes dans le courant de l'année prochaine. Les développeurs intéressés peuvent aussi avoir accès au client sur GitHub. Dans les mois à venir, nous nous efforcerons d'ajouter d'autres routeurs à la liste.

02 Combien de réseaux utilisant Commotion sont disponibles dans le monde ? Pouvez-vous nous citer l'exemple d'un réseau d'importance ? Qu'en est-il de la France ?

Commotion est un projet relativement récent. Nous avons travaillé avec des groupes locaux à Detroit et à Brooklyn ainsi qu'avec des petites communautés dans le monde entier. Il existe de plus

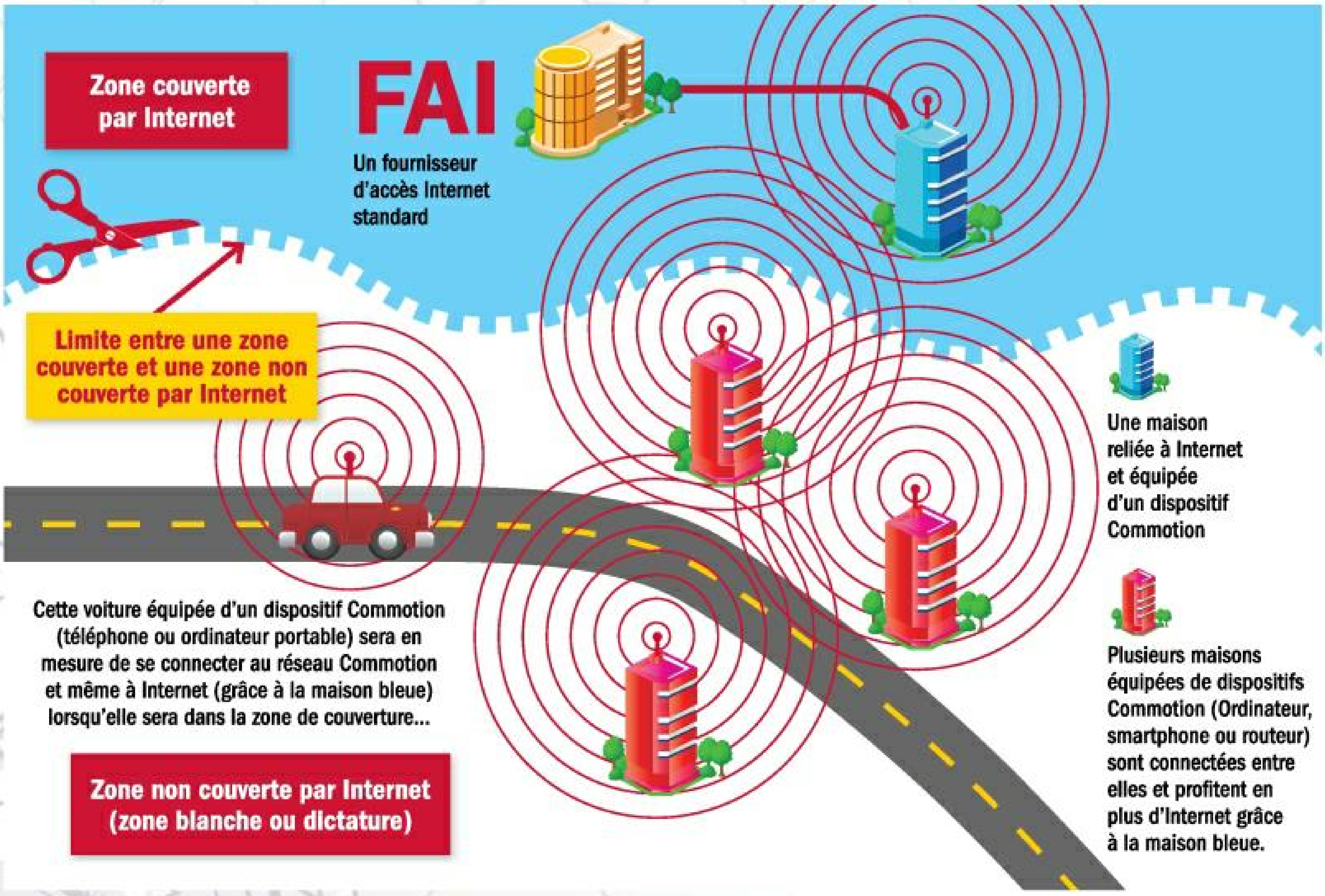
Un exemple de réseau Commotion

CE QU'IL VOUS FAUT

COMMOTION

OÙ LE TROUVER ? : **https://commotionwireless.net**

DIFFICULTÉ : ☠☠☠



vieilles et de plus grandes communautés de réseau sans fil comme Commotion, mais utilisant d'autres variétés de matériels et de logiciels comme Athens Network, Guifi en Espagne, Freifunk, Nepal Wireless, AirJaldi et DEF en Inde, etc. Une autre grosse communauté appelée Altermundi se situe en Argentine. En Europe, le Confine Project (http://confine-project.eu) devient très actif.

03 Où commencer pour un débutant qui souhaiterait créer un réseau communautaire via Commotion ?

L'OTI a élaboré des documents pédagogiques accessibles pour soutenir les organisateurs communautaires à construire des réseaux sans fil. Vous pouvez les trouver ici : www.commotionwireless.net/docs/cck.

04 Les FAI sont souvent méfiant en ce qui concerne ce type de réseau, car cela pourrait signifier moins de clients si une personne avait la possibilité de partager son réseau Wi-Fi avec d'autres. Pas de problèmes avec ces compagnies ?

L'EFF (Electronic Frontier Foundation) a fait un grand travail dans ce domaine. Les FAI locaux sont naturellement plus enclins à supporter notre travail que les FAI de plus grande importance. À Brooklyn, le FAI local Brooklyn Fiber a été d'une grande aide pour notre réseau dans ce secteur et a été un excellent partenaire pour l'organisation locale (Red Hook Initiative).



DARKNET(S) : CE QUE LES MÉDIAS NE VOUS DISENT JAMAIS...

Difficile de se mettre d'accord sur une définition de «darknet». Repaire de «pédo-nazis» pour certains, oasis de liberté pour d'autres, ces couples logiciels/protocoles permettant d'accéder à des parties cachées d'Internet sont en ce moment dans l'œil du cyclone. Alors pourquoi ces réseaux sont-ils nécessaires, qu'y trouve-t-on et qui les utilisent ?

Lors d'une émission sur France Culture de novembre 2013, deux journalistes spécialisés et Jérémie Zimmermann de la Quadrature du Net ont presque passé la moitié de l'émission à essayer de définir le terme «darknet». Pas facile en effet de trouver un terrain d'entente. On parle de darknet au singulier ou au pluriel, tandis que pour d'autres ce terme est une invention de journaliste pour parler d'un secteur Internet qui n'est pas référencé par Google ou Microsoft. En effet, pour 90 % des gens Internet c'est Facebook, YouTube, Google ou Bing, mais il y a aussi toutes les données auxquelles tous les utilisateurs ne peuvent accéder (base de données, FTP, réseau d'entreprise, topsites, archives diverses, etc.) que certains appellent le Deep Web ou Web caché. Darknet c'est encore autre chose...

SANS ANONYMAT, LA VIE PRIVÉE EST MENACÉE

Derrière le terme darknet se cachent juste divers couples logiciel/protocole conçus pour différentes utilisations : téléchargement, surf anonyme, communication, partage, etc. Vous avez sans doute déjà entendu parler de Freenet, Tor ou I2P. Les médias dominants nous vendent le concept du darknet comme un réseau caché où sévissent les vendeurs de drogue, les assassins, les nazis et les pédophiles. En premier lieu, il faut savoir que les darknets ne sont pas si cachés que ça. Le temps d'une installation et vous

LES «DARKNETS» ET LEURS CARACTÉRISTIQUES

	Utilisation principale (comprenant les logiciels fournis	Utilisation secondaire (via des plugins ou des versions modifiées)	À savoir	Licence	Date de création
Tor	Surf anonyme, téléchargement, services cachés (sites en .onion)	Échange de fichiers (via OnionShare, voir page 28)	Pas de solution intégrée pour la messagerie, mais le logiciel Bitmessage est issu du projet Tor	BSD	2002
Freenet	Freesites (l'équivalent des services cachés de Tor), téléchargement, forums, échange de fichiers entre amis	Courrier électronique (Freemail)	Freenet ne peut être utilisé comme solution d'anonymisation pour surfer sur l'Internet «visible»	GNU GPL	2000 (changement de cap en 2008 avec une utilisation mixte F2F-darknet)
I2P	Échange de fichiers P2P résistant à la censure, IRC, courrier électronique, services cachés (eepSites)	Surf anonyme, messagerie instantanée, forum, blog anonyme, stockage de fichiers décentralisé.	I2P est disponible sur d'autres supports comme les appareils Android ou les micro-ordinateurs Raspberry Pi.	Multiple	2003
RetroShare	Échange de fichiers P2P résistant à la censure, courrier électronique, messagerie instantanée, forums		Principalement utilisé pour les échanges de fichiers. Ne peut être utilisé comme solution d'anonymisation pour surfer sur l'Internet «visible»	GNU GPL	2006

êtes connectés à des torsites ou des freesites (des sites «cachés») sans vraiment de connaissances techniques. Pour être et rester anonyme, il faudra malgré tout être vigilant (éviter certains types de fichiers qui peuvent trahir votre IP, ne pas ajouter de plugin au navigateur, etc.). Par contre, il est vrai que parmi ces sites Internet cachés, on trouve tout un tas de choses affolantes et illégales. Mais ces sites ne sont que la conséquence du modèle d'Internet qu'essayent de nous imposer



Goolge/Facebook/Microsoft et les grosses compagnies du Net.

LES MÉDIAS FOCALISENT SUR LA PARTIE ÉMERGÉE DE L'ICEBERG

Les darknets sont la réponse des incursions de ces entreprises dans notre vie privée et nous ne parlons même pas de la NSA et autres services secrets. Ces réseaux dans le réseau permettent d'échapper à la traçabilité quel qu'en soit la raison. Notons aussi que sans anonymat il n'y aurait pas de sources pour les journalistes. C'est pourquoi le New Yorker propose aux internautes des espaces chiffrés utilisant la technologie Tor où n'importe quelle information peut être postée sans crainte. De son côté, Reporter Sans Frontière fournit sur son site un «kit de survie». Sorte de cours accéléré pour journaliste désirant protéger

ses communications. Pourtant, on a souvent entendu à la télévision parler du site Silk Road, sorte d'eBay de la drogue accessible avec le protocole Tor. Selon le FBI, ce site a généré 1,2 milliard sur 3 ans alors que le marché mondial de la drogue pèse plus de 320 milliards par an. Une goutte d'eau ! Silk Road vend aussi des armes ? Mon Dieu ! Aux USA, il suffit d'aller au supermarché pour s'équiper… Faire passer Tor ou Freenet pour des repaires exclusivement remplis de brigands fait le jeu du combat contre le respect de la vie privée et c'est exactement ce que font les reportages sensationnalistes de M6 ou de France Télévision. Alors, qui utilise ces outils ? On trouve un peu de tout. Comme dans la vraie vie. Des criminels, des arnaqueurs et des paranos. Mais aussi des gens comme vous et moi qui en ont marre de la surveillance généralisée sur Internet.

SUR NOTRE CD
Sur notre CD, retrouvez l'article sur Tor que nous avons réalisé dans le dernier numéro…



TorBrowser, le navigateur «compagnon» de Tor est une version modifiée de Firefox. Attention, n'installez pas de plugin sous peine de voir votre anonymat compromis !

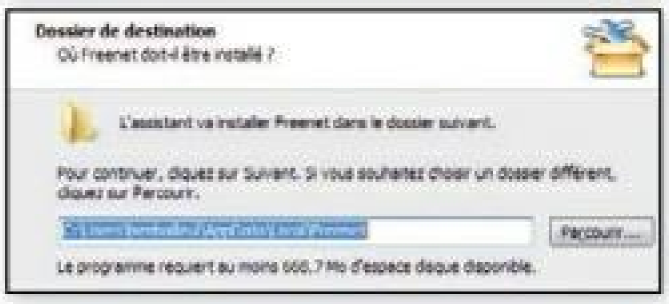
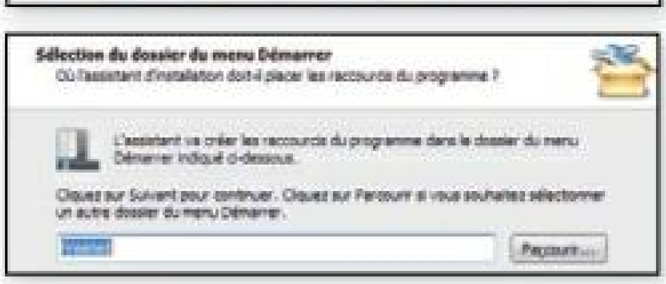
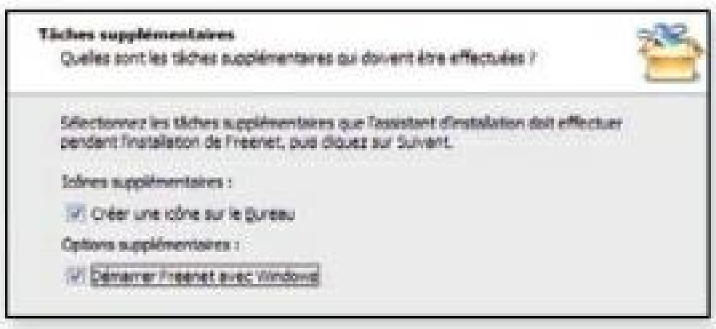
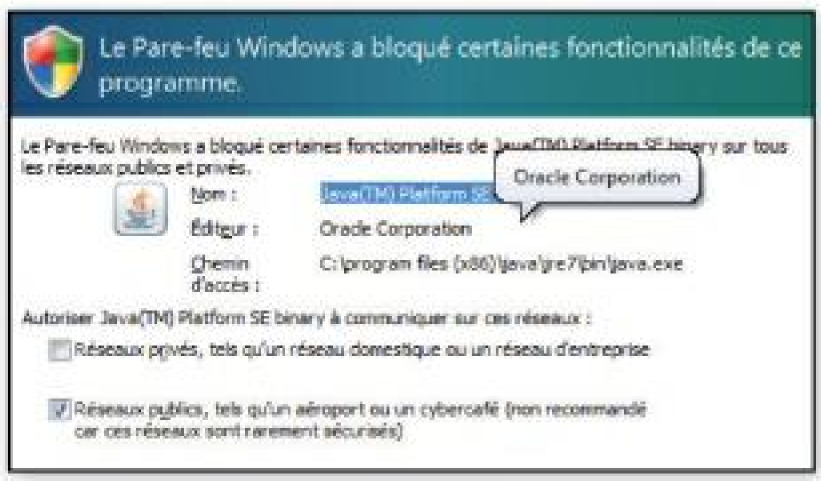
COMMENT ÇA MARCHE ?

Chaque couple logiciel/protocole dispose de ses propres techniques pour garantir un anonymat relatif à ses utilisateurs. Relatif, car il n'existe pas de solution 100 % sûre. Freenet repose sur une architecture basée autour d'amis de confiance. Si vous n'avez pas d'ami déjà dans le réseau, les recherches seront plus laborieuses et le contenu difficilement accessible. Il faudra au fur et à mesure étoffer votre réseau. Lorsque vous aurez au moins 5 amis qui sont en ligne en même temps, votre niveau de sécurité sera suffisamment élevé pour assurer un anonymat presque parfait et avoir accès à un plus grand pan du réseau. Le contenu est chiffré et stocké dans un espace disponible sur chaque ordinateur du réseau. Vous ne savez donc pas quel contenu vous hébergez. Chez Tor, le système repose sur des nœuds, des serveurs qui transportent les paquets d'information de manière anonyme. Seul le nœud «de sortie» vers l'Internet visible est connu. Il est donc difficile de «remonter» l'information. Aujourd'hui, les ennemis de Tor concentrent leur force sur ces nœuds de sortie en essayant de les identifier, mais les développeurs ont plus d'un tour dans leur sac. Les autres darknets utilisent des systèmes similaires : entre décentralisation, chiffrement et routage complexe des paquets.

PAS À PAS →

Vos débuts avec Freenet

CE QU'IL VOUS FAUT
FREENET
OÙ LE TROUVER ? : **https://freenetproject.org**
DIFFICULTÉ : ☠☠☠

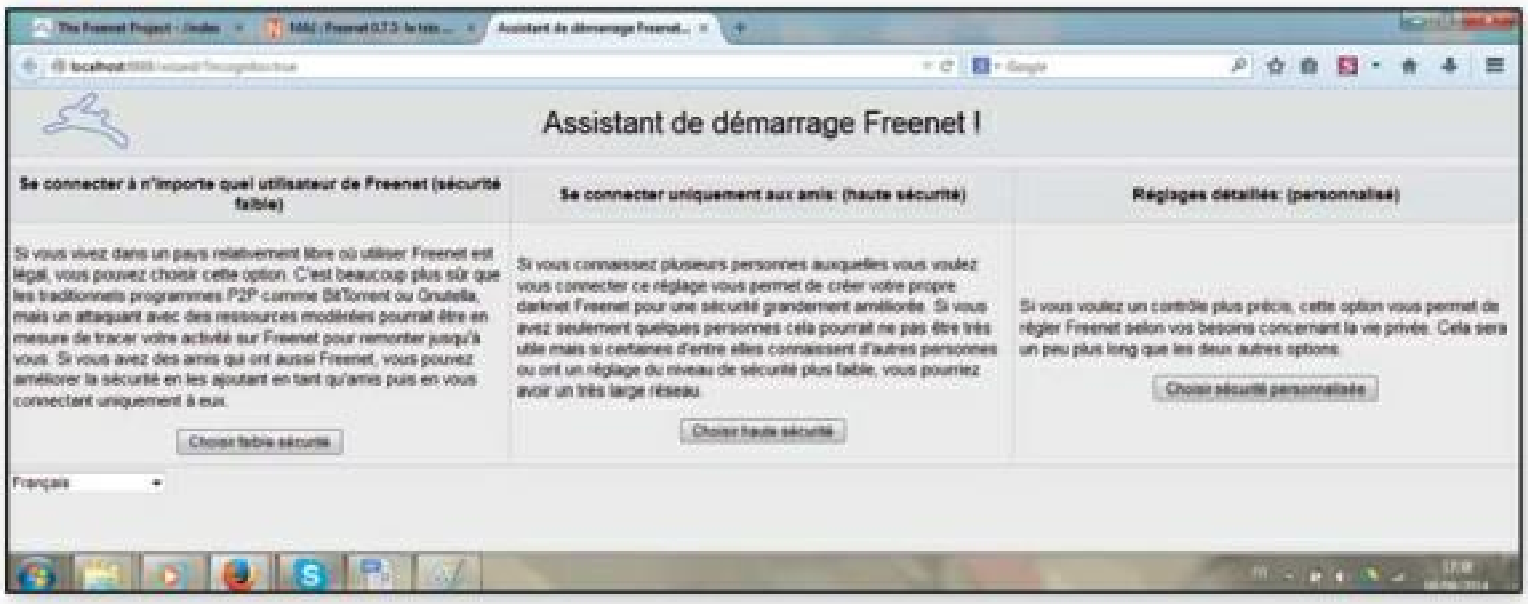
01 L'INSCRIPTION

Freenet s'installe comme un logiciel «normal». Vous devrez choisir son emplacement, s'il doit démarrer en même temps que le système et autoriser l'accès à travers le pare-feu. Dans la zone de notification (en bas à droite à côté de l'horloge Windows) faites un clic sur le lapin puis **Open Freenet**. Le logiciel affichera une interface spécifique dans votre navigateur lors de son lancement. La première fois, l'assistant de connexion vous demandera de choisir le type de démarrage.



02 DES DÉBUTS LABORIEUX

Il faut savoir que Freenet repose sur une architecture basée sur vos relations avec des «amis de confiance». Si vous n'avez pas d'ami déjà dans le réseau, les recherches seront plus laborieuses, le contenu difficilement accessible et la sécurité sera moindre. Il faudra au fur et à mesure étoffer votre réseau. Lorsque vous aurez au moins 5 amis qui sont en ligne en même temps, votre niveau de sécurité sera suffisamment élevé pour assurer un anonymat presque parfait.



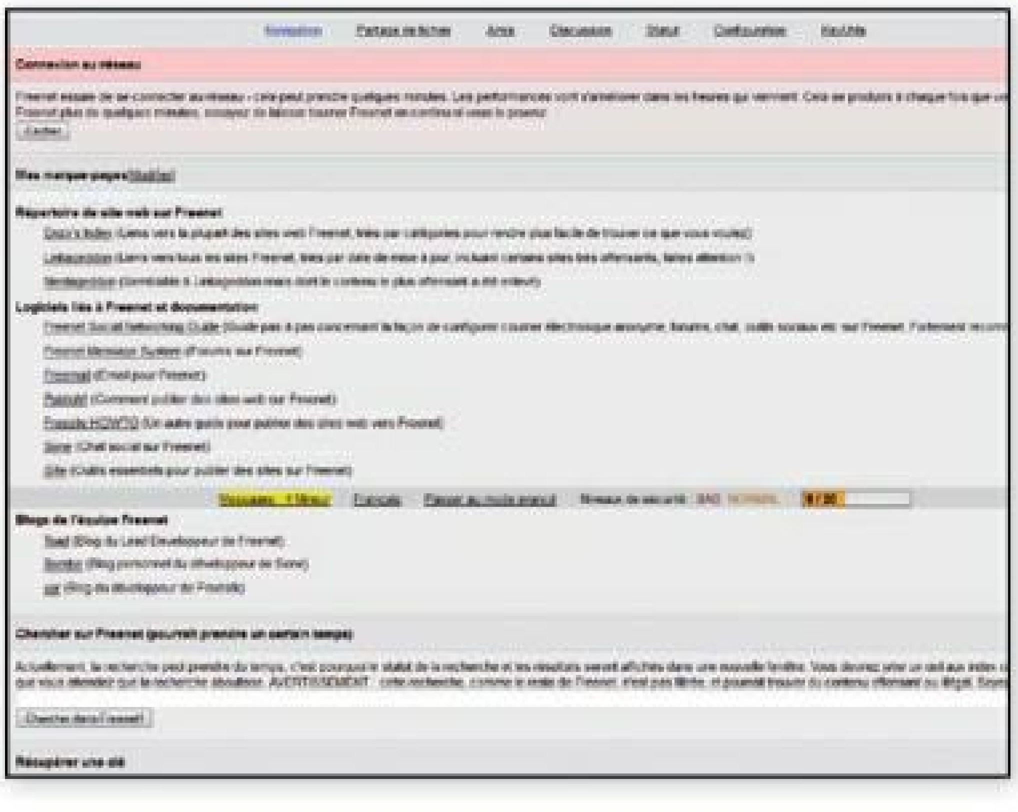
03 VOTRE HISTORIQUE PEUT VOUS TRAHIR



De même, il est conseillé d'utiliser un navigateur séparé pour Freenet, car même si le protocole est sécurisé, l'historique pourrait vous trahir. Le plus simple est d'ouvrir un mode de navigation privé avec Firefox par exemple. Freenet vous demandera ensuite de choisir la taille du répertoire du datastore. C'est l'endroit où seront stockées les données faisant partie de Freenet (puisque chaque utilisateur héberge une partie du contenu). Bien sûr, ce datastore est chiffré de sorte que vous ne savez pas quel contenu vous hébergez.

04 LA PAGE D'ACCUEIL

Mais ce n'est pas encore fini puisqu'il fournit des informations concernant votre débit Internet (limite, vitesse, etc.) pour enfin arriver à la page d'accueil. Sur cette dernière, vous trouverez des index des sites Freenet pour commencer à surfer sans pour autant faire de recherche sur le moteur (très longue et peu précises lorsque vous n'êtes encore qu'en sécurité minimum) ainsi que des outils pour communiquer ou vous familiariser avec Freenet.





05 LES INDEX ET LES AUTRES ONGLETS

Les index sont des pages entières de liens vers des sites ou des documents du réseau. Vous constaterez que la navigation est un peu plus lente que sur l'Internet «normal» et qu'il vous faudra un peu de patience avant de trouver de que vous rechercher. Dans les autres onglets, vous pourrez ajouter des amis pour étoffer votre réseau, partager des fichiers ou configurer Freenet. Lorsque vous cliquerez sur un site, une barre de progression s'affichera.

06 TÉLÉCHARGEMENTS DANGEREUX ?

Pour les téléchargements, c'est un peu plus complexe, car certains types de fichiers peuvent trahir votre IP. Il pourrait s'agir d'un fichier émanant d'un nœud malicieux. Il est donc recommandé de ne rien télécharger si vous êtes encore en sécurité minimum. Si vous souhaitez prendre le risque, vous pouvez toujours choisir de forcer le navigateur à télécharger le fichier puis le consulter hors ligne (complètement déconnecté d'Internet).



DARKNET(S) : QU'EST-CE QU'ON Y TROUVE ?



Pour se faire un avis sur le contenu des darkets, nous avons donc décidé de tester nous-même Tor et Freenet pendant un mois. Sans a priori, nous nous sommes lancé dans l'exploration d'une partie d'Internet faisant couler beaucoup d'encre.





UN MOIS SUR TOR ET FREENET


C'thulhu

Solutions to Common Problems! We are an organized criminal group, former soldiers and mercenaries from the FFL, highly-skilled, with military experience of more than five years. We can perform hits all around the world.

Murder Types	Low Rank	Medium Rank	High Rank and Political
Regular	$45,000	$90,000	$180,000
Missing in action	$60,000	$120,000	$240,000
Death in accident	$75,000	$150,000	$300,000
Criple Types	**Low Rank**	**Medium Rank**	**High Rank and Political**
Regular	$12,000	$24,000	$48,000
Uglify	$18,000	$36,000	$72,000
Two Hands	$24,000	$48,000	$96,000
Paralyse	$30,000	$60,000	$120,000
Rape	**Low Rank**	**Medium Rank**	**High Rank and Political**
Regular	$7,000	$14,000	$28,000
Under age	$21,000	$42,000	$84,000
Bombing	**Low Rank**	**Medium Rank**	**High Rank and Political**
Simple	$5,000	$10,000	$20,000
Complex	$10,000	$20,000	$40,000

C'thulhu se présente comme une organisation criminelle formée d'anciens soldats et mercenaires. Le meurtre à la carte !

Le fonctionnement de Tor et de Freenet est différent puisque Tor offre l'anonymat sur l'Internet de monsieur tout le monde en plus de sites «cachés» tandis que Freenet est plus renfermé sur lui-même. Tor s'installe sans encombre et distille des astuces pour ne pas trahir son anonymat. Le protocole est fourni avec TorBrowser, un navigateur basé sur Firefox. Depuis ce dernier, il est donc possible de surfer sur tout l'Internet sans pour autant dévoiler qui vous êtes. Par contre pour les «services cachés», les fameux torsites dont les adresses se terminent en .onion, il a fallu fureter un peu sur Google.

TOR OUVERT AU MONDE, FREENET PLUS RENFERMÉ

En parallèle, nous avons essayé Freenet. Ici, c'est un peu plus austère et lent. Une fois que le logiciel est installé, il faudra vous connecter depuis votre navigateur (Freenet conseille un logiciel qui autorise une navigation privée). La page d'accueil Freenet FProxy propose de la documentation sur le réseau, l'accès au blog de l'équipe de développement, un moteur de recherche et des répertoires de sites. Ces index proposent un petit tour d'horizon du réseau, mais permettent aussi d'éviter trop

de frustration pour les nouveaux arrivants. En effet, sur Freenet, il faut élargir son réseau. Sans ami de confiance connecté, non seulement votre niveau de sécurité n'est pas très élevé, mais l'accès au contenu est difficile. Une simple recherche sur le moteur peut prendre près d'une heure avec des résultats souvent décevants. En attentant de nous faire des contacts, nous optons donc pour la visite des index...

WELCOME TO THE JUNGLE

Ce qui frappe en premier c'est la quantité de contenus illégaux. En deux clics, vous voilà dans une zone de non-droit d'Internet. On compte environ un tiers de porno (dont une bonne partie de pédopornographie et d'autres trucs louches), un autre tiers de contenu illégal (culture de drogue, négationnisme, numéro de carte bancaire, comment faire un petit engin explosif, etc.) et un dernier tiers de sites inclassables. Dans cette catégorie, on trouve des sites contre l'exploitation animale avec des emplacements de ferme à fourrure (et des détails concernant la sécurité des installations), des sites où l'on peut télécharger des livres interdits (de Mein Kampf à des ouvrages pour réussir son suicide). Sur Tor, c'est le même constat. 80 % des services cachés de la liste que nous avons trouvé sur Google ne comporte que du contenu louche : pédophilie, vente d'arme, fausse monnaie, faux papiers, etc. C'est à ce moment que nous constatons que si les médias se focalisent sur le contenu illégal des darknets c'est parce qu'il est très facile de le trouver. Sur Tor, et dès le premier jour, nous avons trouvé un site effroyable qui vous donne la possibilité de commanditer un meurtre, un passage à tabac ou la pose d'une bombe. Les prix sont variables en fonction de la cible. Sachez donc qu'il vous



Qu'il s'agisse de vendre, acheter ou apprendre à cultiver de la drogue, Freenet et Tor sont très riche en contenu.



Tout un tas de documents contrefaits, de faux billets et des armes...

COMMENT FONCTIONNE L'ÉCONOMIE DES DARKNETS ?

En se demandant comment ces sites de criminels (drogue, assassinat ou hacking) pouvaient fonctionner ou s'il n'était pas tout simplement des faux, des pièges de la police ou des escroqueries organisées, nous avons découvert le concept d'«escrow». Il s'agit d'intermédiaires entre acheteur/vendeur ou commanditaire/exécutant. Les transactions sont payées en Bitcoin et ceux qui proposent un service ne sont payés par l'escrow que lorsque le demandeur donne le feu vert. Bien sûr la plupart du temps l'intermédiaire prend une petite part du gâteau.

en coûtera 45 000 dollars pour faire abattre votre voisin ou 18 000 dollars pour défigurer votre ex.

AU BOUT DE QUELQUES JOURS, FINALEMENT...

Après avoir vu tout ce que les darkets avaient à offrir de pire, nous nous sommes mis à chercher ce qu'ils avaient à offrir de meilleur. De forum en forum et après avoir trouvé des moteurs de recherche de site TOR, nous avons enfin pu trouver autre chose que des nazis et de la drogue. Avec Freenet et l'ajout de deux amis, le contenu est plus riche. Même si la sécurité est encore au niveau le plus bas, les recherches sont plus rapides et moins décevantes. Il nous a fallu plusieurs jours pour voir un aspect plus respectable de ces deux protocoles : des blogs sur la liberté d'expression ou sur la promotion de la cryptographie, des sites d'indépendantistes de tous poils ou qui dénoncent des abus de pouvoir policiers, des photos de la situation en Ukraine, des documents sur le régime syrien ou sur la guerre en Afghanistan, des blogs contre le régime chinois ou parlant des événements de la place Tian'anmen, etc. *Envoyé Spécial* et *Zone Interdite* sont restés à la case «nazi». Il fallait jeter les dés encore quelques tours...



Sur ce site, vous pouvez louer les services d'un hacker. Pour 200 €, vous pouvez paralyser le site de votre concurrent ou le faire passer pour un pédophile aux yeux de la police.











Et finalement, en cherchant bien nous avons trouvé des informations concernant le régime syrien, la guerre en Ukraine et des blogs de dissidents.

Des emplacements précis de fermes à fourrures particulièrement recherchés par les défenseurs de la cause animale.


TÉLÉCHARGER
// STREAMING
MAGAZINE INTERDIT
N°10
DOWN LOAD
+540 SOFTS & SERVICES OFFERTS SUR NOTRE CD
JANV. / MARS 2015
TÉLÉCHARGEMENT & MULTIMÉDIA
LE GUIDE DU
TÉLÉCHARGEMENT DIRECT
» BEST OF SITES
» DOWNLOADS RAPIDES & ILLIMITÉS
FILMS & SÉRIES
POPCORN TIME
LE RETOUR DU ROI
BON PLAN
Les sites où la MUSIQUE est MOINS CHÈRE !
+ DES DIZAINES DE TUTOS!
MOBILE : Top astuces pour TRANSFÉRER sa MUSIQUE
Enregistrez le STREAM
SOUS-TITRES automatiques !
ÉMULEZ avec ROMSTATION
MOBILE : Dopez le stockage !
BEST-OF > Services Musique
BEST-OF > Services Vidéo
+ CD OFFERT !
N°10
DOWN LOAD
LE KIT COMPLET
© 2015 ID PRESSE
DOWNLOAD
STREAMING
MOBILES
TROUSSE À OUTILS
TUTOS & BONS PLANS
540 LOGICIELS & SERVICES GRATUITS
+2 MAGAZINES COMPLETS OFFERTS !
CD GRATUIT POUR WINDOWS
CHEZ VOTRE MARCHAND DE JOURNAUX !

SAUVEGARDE ET SYNCHRONISATION FACILES !



Ceux qui ont déjà expérimenté la perte de données importantes savent à quel point une sauvegarde peut changer la vie. Pour éviter que cette manipulation ne soit trop pénible, FullSync permet d'automatiser ses backups ou de les gérer à distance. Vous n'aurez plus d'excuses lors de votre prochain gros pépin...

Pour que cette démarche soit la plus simple possible et éviter de perdre des données dans la manœuvre (ce qui serait un comble !), nous avons choisi de vous présenter FullSync. Ce dernier est simple à prendre en main et est aussi à l'aise avec des sauvegardes simples, incrémentielles ou avec de la synchronisation de fichiers (dans un ou deux sens). Plus fort, vous pourrez très bien automatiser des sauvegardes depuis et vers des répertoires locaux, du FTP, du SFTP ou des partages Windows (SMB).

DÉBUTANTS OU EXPERTS !

Le mode Publish/Update vous permettra même de mettre à jour un site Web à partir d'une copie locale. Bien sûr, tout est paramétrable dans le temps (un oubli est si vite arrivé) et vous disposerez aussi de filtre pour exclure certains fichiers. Attention, contrairement à Cobian Backup que nous vous avons présenté dans notre numéro 18, FullSync ne comporte pas de module de compression ou de chiffrement.



Très clair, FullSync fonctionne sous Java. Il vous faudra donc la dernière version de ce logiciel pour en profiter...

Il convient donc parfaitement aux débutants qui veulent stocker des fichiers non sensibles ou aux experts qui pourront utiliser FullSync pour des sauvegardes sur Internet ou des mises à jour de sites Internet.

LEXIQUE

*** SAUVEGARDE INCRÉMENTIELLE :** Une sauvegarde en mode incrémentiel permet de ne sauvegarder que le contenu modifié depuis la dernière sauvegarde. C'est un gain de temps et de place sur le disque dur.

1001101010001000101010110010010010101000100101001010010101010010000111010101010

PAS À PAS

Un exemple concret avec FullSync

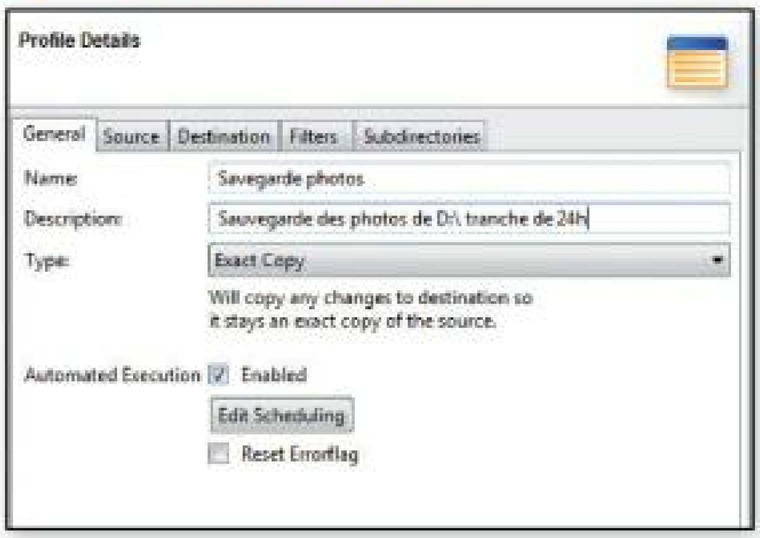
CE QU'IL VOUS FAUT

FULLSYNC

OÙ LE TROUVER ? : **http://fullsync.sourceforge.net**

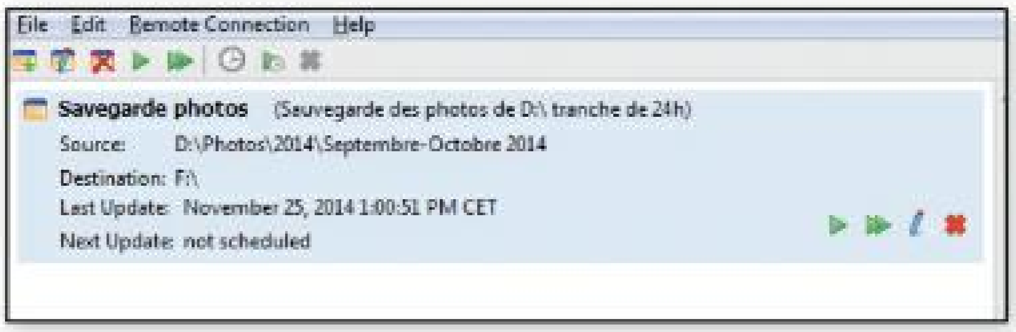
DIFFICULTÉ :

01 LE «PROFIL»



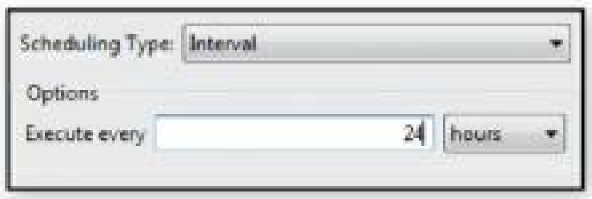
Avant de commencer, sachez que FullSync est aussi disponible dans une version ne nécessitant pas d'installation. Dès l'ouverture, il faudra se créer un «profil» (**New Profile**). Il s'agit en fait d'éditer votre sauvegarde. Dans notre exemple, nous allons faire une sauvegarde de nos photos sur un disque dur externe toutes les 24 heures. Après avoir entré un nom et une description, il faudra choisir le **Type**.

02 4 CHOIX DE SAUVEGARDER/ SYNCHRONISATION



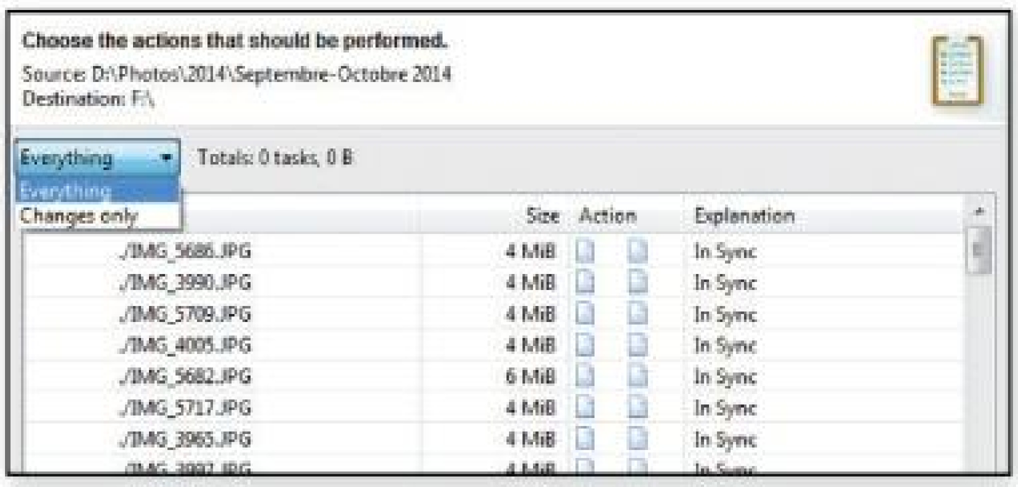
Vous aurez 4 choix. **Publish/Update** est utilisé pour mettre à jour un site Web à partir d'une copie locale d'un serveur distant tandis que **Backup Copy** va tout sauvegarder sans effacer quoi que ce soit dans le dossier de destination. **Exact Copy** est la solution idéale pour nos photos puisque tous les changements seront pris en compte, y compris les suppressions (vous n'aurez pas à vous encombrer des versions antérieures de photos). Enfin, **Two Way Sync** va comparer la source et la destination puis ira copier les fichiers plus récents d'un côté comme de l'autre (attention, car les versions antérieures seront écrasées !).

03 AUTOMATISATION



Plus bas, vous pourrez aussi paramétrer une exécution automatique. Cochez **Enabled** et faites **Edit Scheduling**. Ici, vous pourrez régler un intervalle ou et date précise (**Crontab**). Validez et dirigez-vous ensuite vers les onglets **Source et Destination**. Dans notre cas, nous mettrons file dans protocole puisqu'il s'agit d'une sauvegarde locale, mais vous pouvez aussi sauvegarder vers et depuis un serveur FTP, SFTP et SMB. Dans Path, il faudra mettre un chemin (à la fois dans **Source et Destination**). Notez que FullSync permet de sauvegarder ou synchroniser des dossiers même si la source et la destination sont toutes deux distantes (de serveur à serveur). Les autres onglets servent à filtrer des dossiers ou fichiers que vous ne voulez pas sauvegarder (filtres par nom, taille, date de modification, etc.).

04 C'EST TOUT !



Après avoir validé, vous pourrez soit commencer votre première sauvegarde (même si ce n'est pas le moment prévu par vos planifications) en cliquant sur le triangle vert. Vous pouvez aussi vous contenter de suivre votre planification en faisant **Start Scheduler**. Notez que lorsque vous réaliserez votre sauvegarde dans certains modes pour la seconde fois, le logiciel vous demandera si vous voulez tout re-sauvegarder ou si vous ne désirez sauvegarder que les changements (sauvegarde incrémentielle).

DERNIÈRE MINUTE !



Dans **Edit>Preference**, vous pourrez régler la langue française pour l'interface. Notez aussi que pour que FullSync agisse même lorsque vous n'êtes pas là pour surveiller, il faudra qu'il soit en route sur votre PC. Il est possible de «réveiller» le logiciel dans les préférences à **Autostart Scheduler (Démarrer automatiquement la planification)**.

SUR NOTRE CD

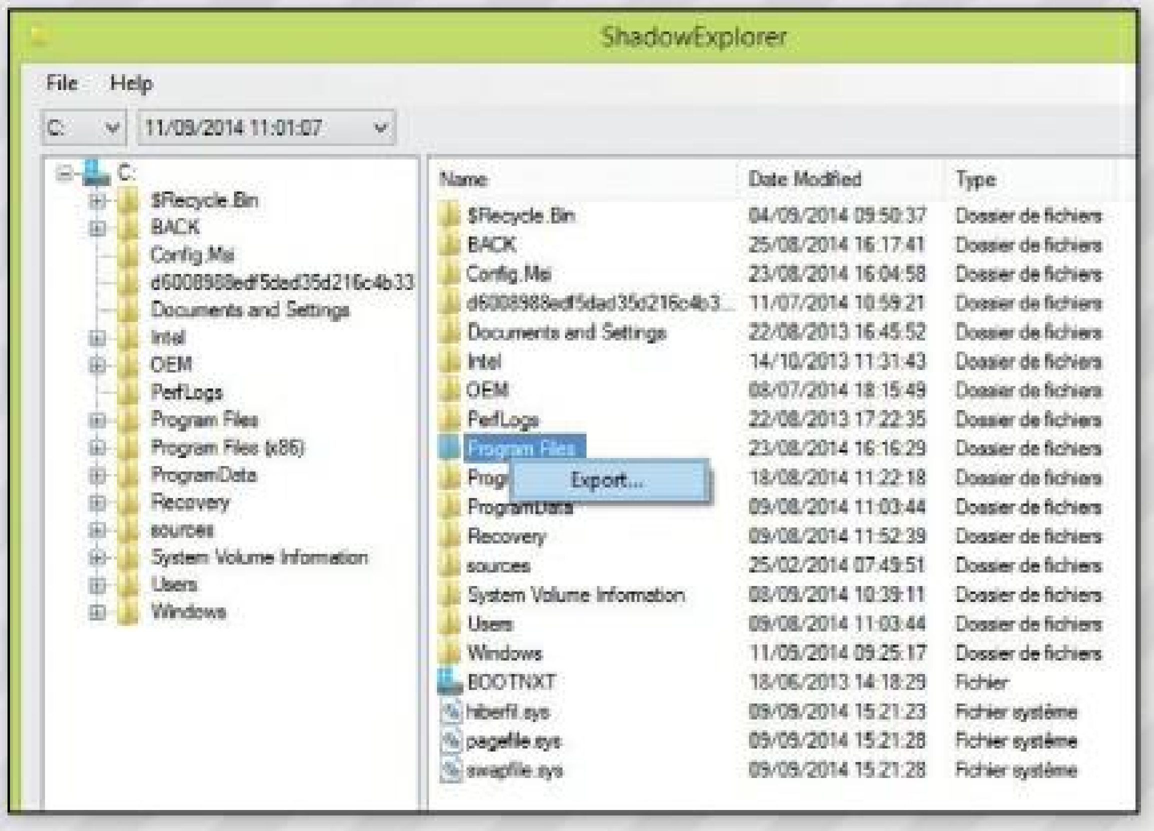
Sur notre CD, retrouvez notre précédent article concernant le logiciel Cobian Backup. Ce dernier permet de faire des sauvegardes standards ou incrémentielles. Il prend aussi en charge le chiffrement AES 256 bits.

#1 Piocher dans les points de restauration

AVEC SHADOW EXPLORER

Shadow Copy est le module de Windows qui crée les points de restauration. Ces derniers sont utilisés lors d'un problème sur votre système (pour revenir à un état précédent), mais il n'est pas possible de retrouver un seul fichier lorsque vous n'avez qu'une version basique ou familiale de Windows. Pour régler ce problème et éviter de tout restaurer, il faudra utiliser Shadow Explorer. Il vous suffira juste de démarrer le programme puis de choisir votre lettre de volume. Choisissez la date du point de restauration puis une fois que vous avez localisé votre fichier, il n'y a plus qu'à faire un clic droit dessus et de choisir **Export**... Votre fichier sera alors disponible dans le système sans pour autant revenir à votre ancien point de restauration.

Lien: **https://spideroak.com**





#2 Débarrassez-vous des Adwares

AVEC ADWCLEANER

Après une installation, vous vous rendez compte que des publicités s'affichent de manière intempestive ou que vous vous retrouvez avec des barres de recherche dans votre navigateur ? Le problème c'est que ces indésirables ne sont pas considérés comme des virus. Pour s'en débarrasser, AdwCleaner est une solution de choix. Sans nécessiter d'installation, AdwCleaner va partir à la recherche des saletés qui se sont invitées dans vos fichiers, base de registre ou navigateurs (adware, toolbar, spyware, etc.) en faisant juste **Scanner**. Lorsqu'il aura détecté des éléments, il suffira de cocher les cases correspondantes et de décider de la marche à suivre : nettoyage, mise en quarantaine ou désinstallation.

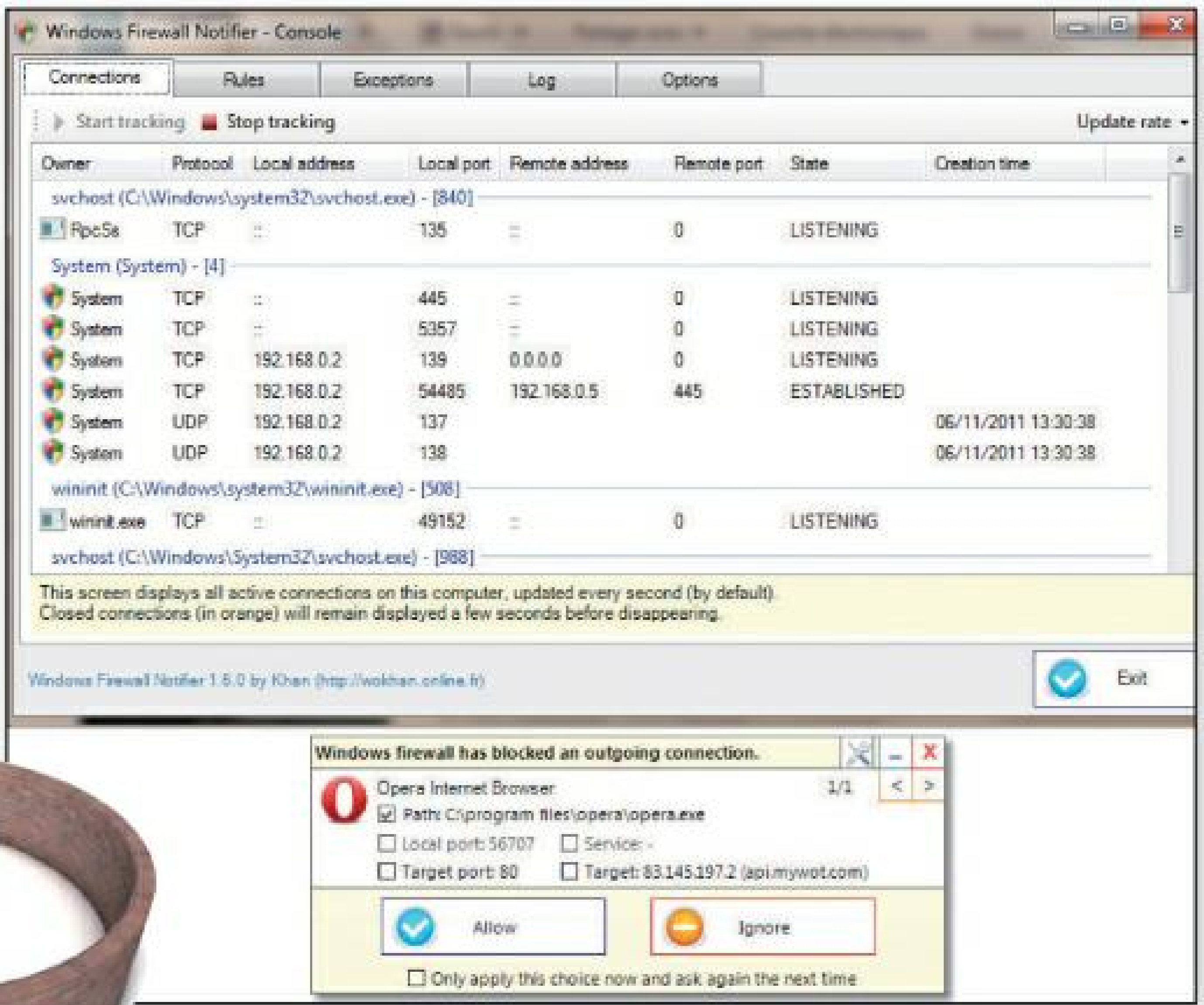
Lien: **http://goo.gl/uPRf2M**

#3 Gérer votre pare-feu comme un pro

AVEC WINDOWS FIREWALL NOTIFIER

Windows Firewall Notifier est le complément idéal de votre pare-feu sous Windows. Il permet d'activer la surveillance des connexions sortantes (ce que ne proposent pas toutes les versions de Windows par défaut), de gérer les connexions en temps réel et d'activer la journalisation des connexions sortantes du pare-feu Windows.
Le logiciel ne tourne pas en permanence au sein du système, mais il crée une tâche planifiée liée aux événements du pare-feu : une fois activé, le logiciel fera apparaître une notification lorsqu'une application tente de se connecter à Internet alors qu'elle n'y est pas encore autorisée.

Lien: **http://wokhan.online.fr**





#4 Duper les mouchards

AVEC GHOSTERY

Ghostery voit ce qui ne se voit pas sur Internet. Il détecte les mouchards, les balises placées sur les pages Web par les réseaux publicitaires et les scripts qui veulent enregistrer vos activités.



Suivez l'assistant d'installation et choisissez d'activer **Ghostrank**, un module qui va recueillir des données anonymes sur les mouchards pour avertir les autres utilisateurs de Ghostery. Cette extension peut empêcher que les éléments de page qu'il détecte s'exécutent dans votre navigateur. Vous pourrez ainsi contrôler la manière dont le suivi de vos données de navigation est effectué. Attention, car le fait de bloquer les mouchards peut avoir des conséquences inattendues sur les sites visités. Certains peuvent être utiles. À vous de faire le tri dans la liste.

Lien: **http://goo.gl/Rx9GAU**

Lien: **http://goo.gl/5RCXy8**

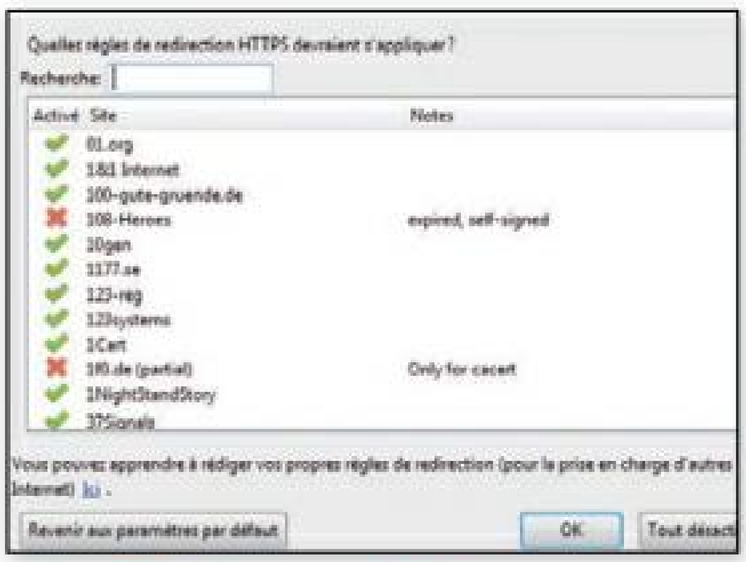
#5 Un clone sécurisé de Tweeter

AVEC TWISTER

Twister est une plateforme de micro-blogging décentralisée et chiffrée basé sur le modèle de Twitter. Son architecture P2P particulière empêche la censure et protège ses utilisateurs des pirates, agences gouvernementales et autres services secrets. Bien sûr votre IP est masquée et il est impossible de supprimer un compte existant. Attention, ce projet en est encore à sa version alpha mais vous pouvez depuis peu télécharger des packs pré-compilés prêts à l'emploi pour Windows et Android.

Lien: **http://twister.net.co**





#6 Un chiffrement forcé

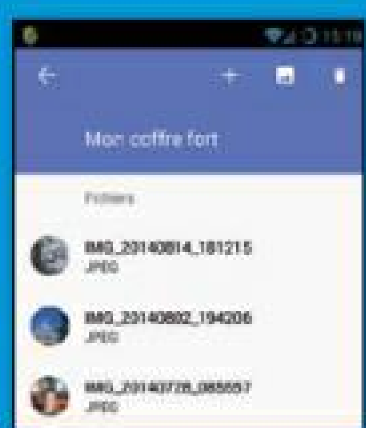
AVEC HTTPS EVERYWHERE

Certains sites ne proposent qu'un support limité du mode sécurisé HTTPS (qui permet, par exemple, de chiffrer les identifiants bancaires lors de vos achats sur Internet ou sur des sites comme ceux de la CAF, PayPal, etc.) Le fameux cadenas qui vous informe de la nature protégée de votre connexion n'est donc plus un indicateur de valeur. Cette extension va tout simplement forcer le site visité à utiliser ce protocole au mieux de sa forme. Cela vous évitera de vous faire pirater des données sensibles ou à éviter le sidejacking lorsque vous vous connectez à un point d'accès Wi-Fi non sécurisé. L'extension est disponible sous Firefox, Chrome, Opera et Android.

Lien: **www.eff.org/https-everywhere**

#7 Chiffrez vos fichiers sous Android

AVEC SECRECY



Si vous souhaitez une solution pour chiffrer les fichiers qui sont sur votre téléphone, vous pouvez toujours le faire avec ES Explorateur (qui propose aussi une option pour masquer) mais si vous préférez une application dédiée pourquoi ne pas essayer Secrecy ? Après avoir créé votre coffre-fort, vous pourrez chiffrer n'importe quel fichier, et pas seulement les photos. Contrairement à ses concurrents, Secrecy ne laisse aucune trace de votre clé dans la mémoire de votre appareil. Raison de plus pour ne pas oublier votre mot de passe...

Lien: **http://goo.gl/gcsAqc**

AUTO-DESTRUCTION DE VOS DONNÉES AVEC KALI LINUX

LEXIQUE

***KALI LINUX :** Anciennement BackTrack, Kali Linux est une distribution spécialisée dans l'audit réseau, le pentesting et plus généralement le hacking. Parmi les outils inclus vous trouverez des logiciels pour cracker des mots de passe, des logiciels de rétro-engineering, des modules pour pénétrer des réseaux sans fil, mais aussi le langage Arduino ou CHIRP (radioamateur). Une vraie mine d'or pour les hackers débutants ou confirmés.

***BOOT :** Le boot est la procédure de démarrage d'un ordinateur. Généralement le PC va «booter» sur le disque dur principal pour charger le système, mais il est possible et parfois nécessaire de booter sur un DVD ou une clé USB pour installer un autre système, lancer un Live CD ou tenter une restauration.

***LIVE CD :** Un live CD est un CD ou un DVD qui contient un système ne nécessitant pas d'installation sur un disque dur. Idéal pour commencer un apprentissage sous Linux sans voir à partitionner son disque et risquer une erreur de manipulation. Dans notre exemple, le Live CD Kali Linux (inclus de base dans l'ISO) nous permettra de restaurer nos données «perdues».





Vous avez lu notre dernier article sur Linux Mageia, mais vous voulez passer à la vitesse supérieure avec Kali Linux ? Bonne idée ! Profitons-en pour aborder une nouvelle fonctionnalité de cette distribution particulière : la mise en place d'un mot de passe «piégé» qui détruira vos données si quelqu'un le tape sur votre PC...

Depuis la version 1.0.6 de Kali Linux, le logiciel Cryptsetup qui sert à chiffrer l'accès au disque dur a été modifié pour permettre aux utilisateurs qui le souhaitent d'ajouter une mesure de sécurité supplémentaire : la mise en place d'un mot de passe alternatif qui détruira vos données au lieu de vous en donner l'accès. Supposons que votre ordinateur est confisqué par une autorité, un ravisseur ou n'importe quelle personne désirant vous torturer pour avoir accès à vos données (et oui, nous lisons beaucoup de romans !). Las de vous faire rentrer des cure-dents sous les ongles, vous cédez et donnez un mot de passe. Pas le mot de passe qui ouvre votre boîte de Pandore mais un mot de passe alternatif, piégé, qui va tout simplement empêcher votre adversaire de récupérer vos données.

JETEZ LA CLÉ DES CHAMPS !

Il ne s'agit pas d'effacer quoi que ce soit, car un formatage serait bien trop long pour être efficace (encore plus si vous vouliez enregistrer des données aléatoires sur votre disque pour éviter une restauration). Le but de la manœuvre sera tout simplement d'effacer le «header», le fichier qui garde en mémoire la clé d'accès chiffrée au contenu du disque. Pour faire simple, les données chiffrées sont toujours là, mais la clé a disparu ! Bien sûr nous verrons comment garder une trace de cette clé pour pouvoir retrouver l'accès aux données (si vous êtes toujours vivant ou sorti de prison !)

METTRE À JOUR VOTRE VIEILLE VERSION DE KALI LINUX

La version patchée de Cryptsetup est disponible d'origine depuis la version 1.0.6 de Kali Linux mais si vous en avez une plus vieille, il suffira d'ouvrir un terminal et de faire :

root@kali-crypto:~# apt-get update

puis

root@kali-crypto:~# apt-get dist-upgrade

010001000101010110010010010101000010 0101001010010101010010000111010101010101110101

Installation de Kali Linux

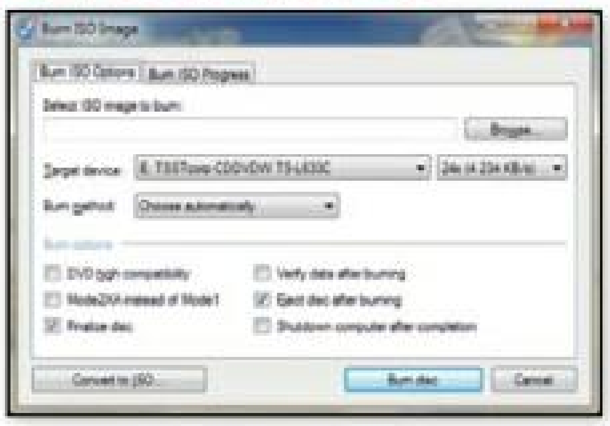
CE QU'IL VOUS FAUT

KALI LINUX

OÙ LE TROUVER ? : **www.kali.org/downloads**

DIFFICULTÉ :

01 L'IMAGE AU FORMAT ISO



En suivant notre lien, téléchargez la dernière version de Kali Linux en fonction de votre type de processeur. Si vous ne savez pas laquelle prendre, optez pour l'**ISO 32 bits**. Ce fichier image devra être gravé sur un DVD vierge avec Windows ou CDBurnerXP. Notez qu'il est possible de l'installer depuis une clé USB en suivant ce tutoriel: **http://goo.gl/FafukJ.**

02 BOOTEZ DEPUIS LE DVD

Une fois que votre DVD est prêt, il faudra juste penser à «booter» sur votre lecteur. Faites **Suppr**, **F1**, **F2** ou **F12** (en fonction de votre modèle de carte mère) juste après avoir allumé le PC et entrez dans le BIOS (**Setup**). Trouvez l'option **Boot Sequence** (qui peut aussi être sélectionnable avant même l'entrée dans les menus) et

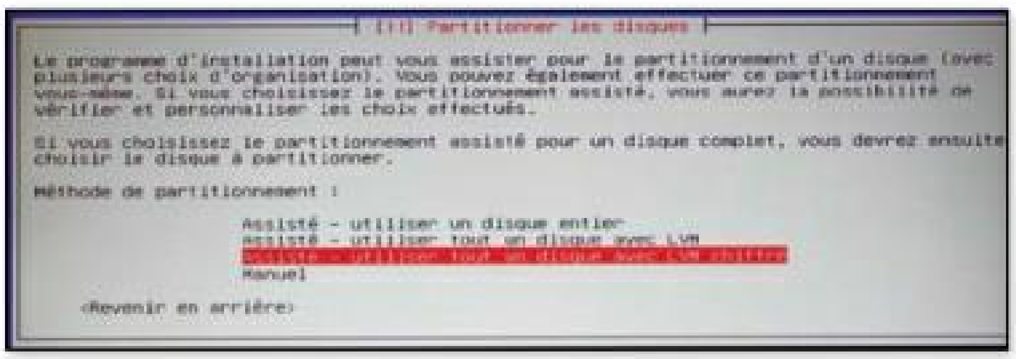


modifiez l'ordre en mettant en premier votre lecteur DVD. Si vous avez des difficultés, consultez la notice de votre carte mère ou jetez un coup d'œil sur Google avec le nom de votre matériel.

03 L'INSTALLATION

Lorsque vous verrez pour la première fois le logo Kali Linux, il faudra choisir **Install** puis paramétrer la langue de l'interface,

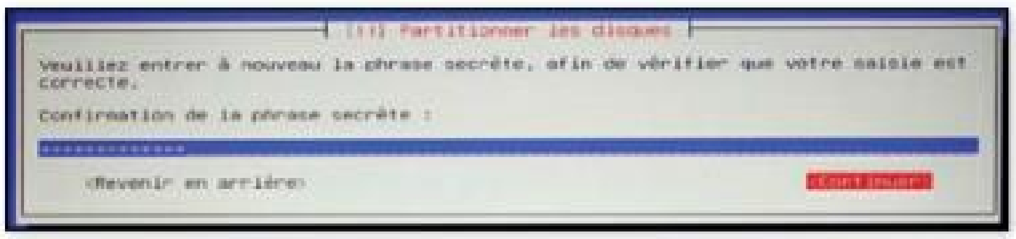




la région du clavier, le mot de passe «root» du superutilisateur, etc. Viendra ensuite le choix du partitionnement. Dans notre cas, nous utiliserons **Tout un disque avec LVM chiffré,** mais vous pourrez aussi le faire manuellement si vous souhaitez garder votre partition Windows (dans ce cas, vous aurez le choix du système au démarrage).

05 LA PHRASE SECRÈTE

On vous demandera ensuite de choisir une phrase secrète pour chiffrer le contenu du disque. Choisissez bien ce sésame et mémorisez-le. Le système va alors commencer à s'installer sur votre disque dur. S'il s'agit du seul système présent sur le disque,



choisissez d'implémenter GRUB, le programme de démarrage. Lorsque les fichiers seront chargés, Kali Linux vous demandera de retirer le DVD d'installation et le PC pourra enfin booter sur le disque dur.

05 UN NOUVEAU MONDE !

Entrez votre phrase secrète lorsqu'on vous la demandera puis le mot de passe superutilisateur pour avoir accès à l'interface. Bienvenu dans Kali Linux! Dans **Applications** vous trouverez les programmes préinstallés classés par types, puis le navigateur d'origine en haut et l'icône pour lancer un terminal juste à sa droite. L'interface n'a rien de bien sorcier, on pourrait même comparer l'organisation à celle de Windows. Prenez possession des lieux!



PAS À PAS →

Mise en place du mot de passe d'auto-destruction

01 LA NOTION DE «KEY SLOT»

Maintenant que vous vous êtes familiarisé avec Kali Linux, voyons comment mettre en place notre dispositif d'auto-destruction des données. Ouvrez un terminal (l'icône en haut près du navigateur) et tapez

root@kali-crypto:~# cryptsetup luksDump /dev/sda5

Vous verrez alors quelque chose comme **Key Slot 0: ENABLED** avec une suite de données. Cela correspond à la «case» où repose votre phrase secrète donnant accès à votre disque dur. Le reste des **Key Slot** doivent normalement être **DISABLED** à ce moment.

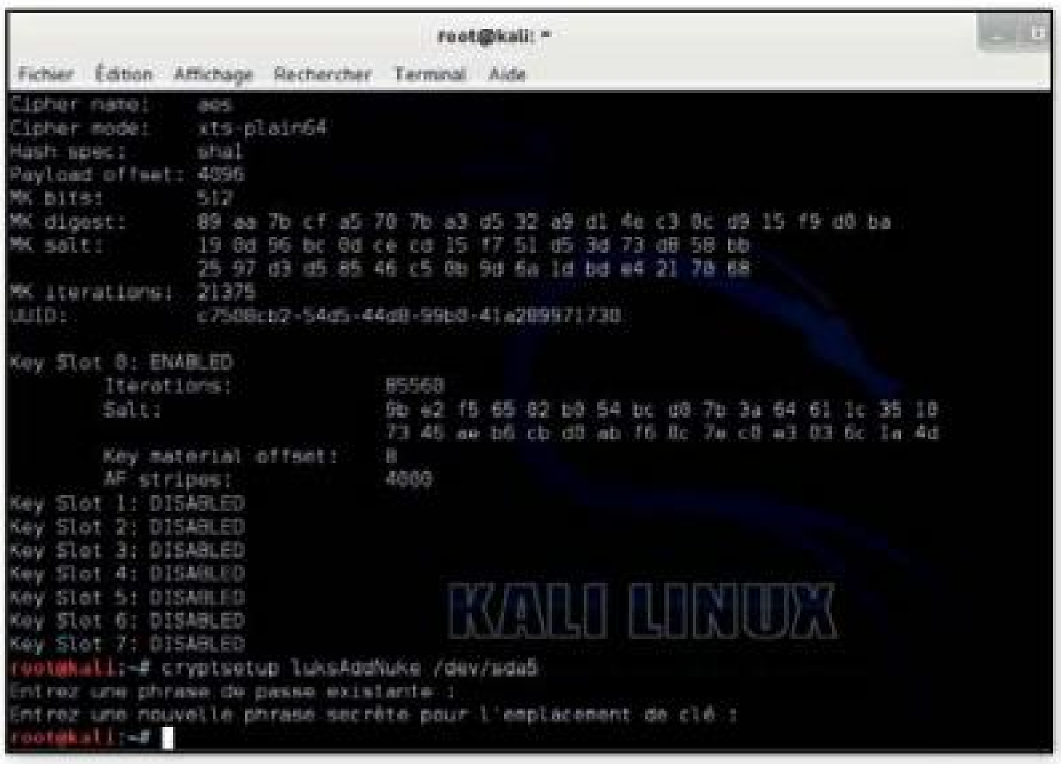


02 VOTRE SÉSAME PIÉGÉ

Ajoutons notre mot de passe d'auto-destruction à cette liste en tapant

root@kali-crypto:~# cryptsetup luksAddNuke /dev/sda5

Kali vous demandera alors de tapez votre phrase secrète d'origine puis la nouvelle, celle qui servira à l'auto-destruction. Vous pouvez



constater les changements en tapant une nouvelle fois

root@kali-crypto:~# cryptsetup luksDump /dev/sda5

Vous verrez alors les **Key Slot 0** et **1** en position **ENABLED**.

02 SAUVEGARDE ET CHIFFREMENT DU HEADER

Sauvegardons alors ces données en tapant

root@kali-crypto:~# cryptsetup luksHeaderBackup --header-backup-file luksheader.back /dev/sda5

puis

root@kali-crypto:~# file luksheader.back

Mais dans notre cas nous souhaitons chiffrer ces données pour les stocker. Nous allons donc le faire avec OpenSSL, inclus dans Kali Linux. Tapez **root@kali-crypto:~# openssl enc -aes-256-cbc -salt -in luksheader.back -out luksheader.back.enc**

puis entrez deux fois un nouveau mot de passe servant exclusivement à chiffrer le header.

Tapez **root@kali-crypto:~# ls -lh luksheader.back***

puis

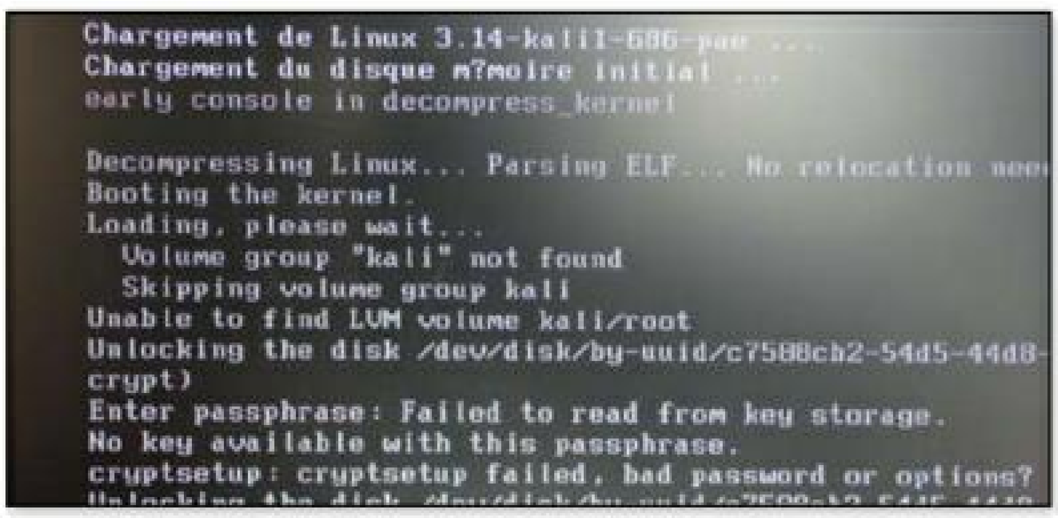
root@kali-crypto:~# file luksheader.back*

Voilà, nous voici avec un fichier «header» **luksheader.back.enc** que vous trouverez dans votre **Dossier Personnel** (**Home** dans la version anglaise du système). Ce fichier devra être placé dans une clé USB pour pouvoir récupérer vos données dans le cas où vous utiliseriez l'option d'auto-destruction.



02 TEST DU DISPOSITIF

Faisons un essai et redémarrons Kali Linux. Lorsque le système vous demandera votre phrase secrète, mettez la seconde, celle qui est «piégée». Kali effacera alors le header et vous perdrez l'accès aux données, même en tapant ensuite votre première phrase secrète. Vos données sont perdues à jamais? Pour les méchants oui, mais pas pour vous!



Récupérez vos données après l'auto-destruction

01 BOOT EN MODE LIVE CD

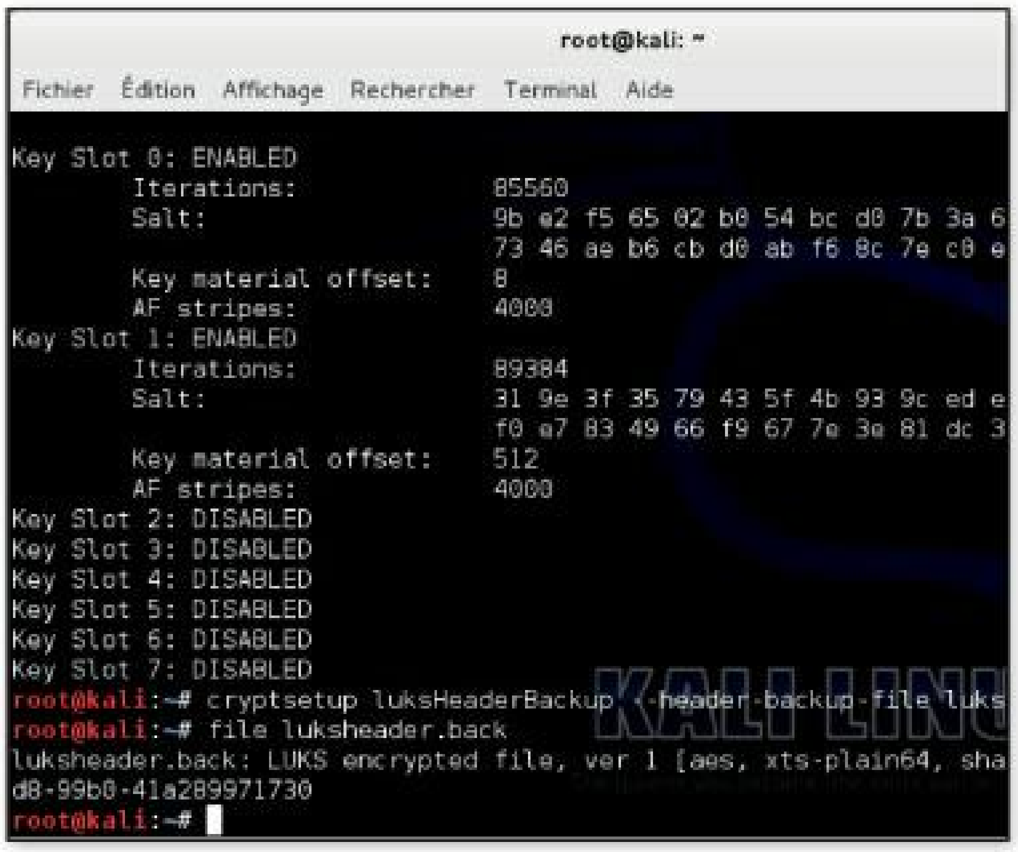
Vous avez volontairement donné la phrase secrète qui tue à vos ravisseurs, la police ou une agence gouvernementale un peu trop curieuse? Vos données ne sont pas perdues pour autantpuisque vous avez placé le fichier **luksheader.back.enc** en lieu sûr! Remettez le DVD d'installation dans votre lecteur, bootez dessus,



mais cette fois-ci choisissez **Live (686-pae)** pour démarrer le Live CD (et surtout pas **Install** !). Kali Linux va se charger en mémoire vive et vous pourrez utiliser toutes ses fonctions sans toutefois avoir encore accès à vos anciennes données.

02 DÉCHIFFREZ VOTRE HEADER

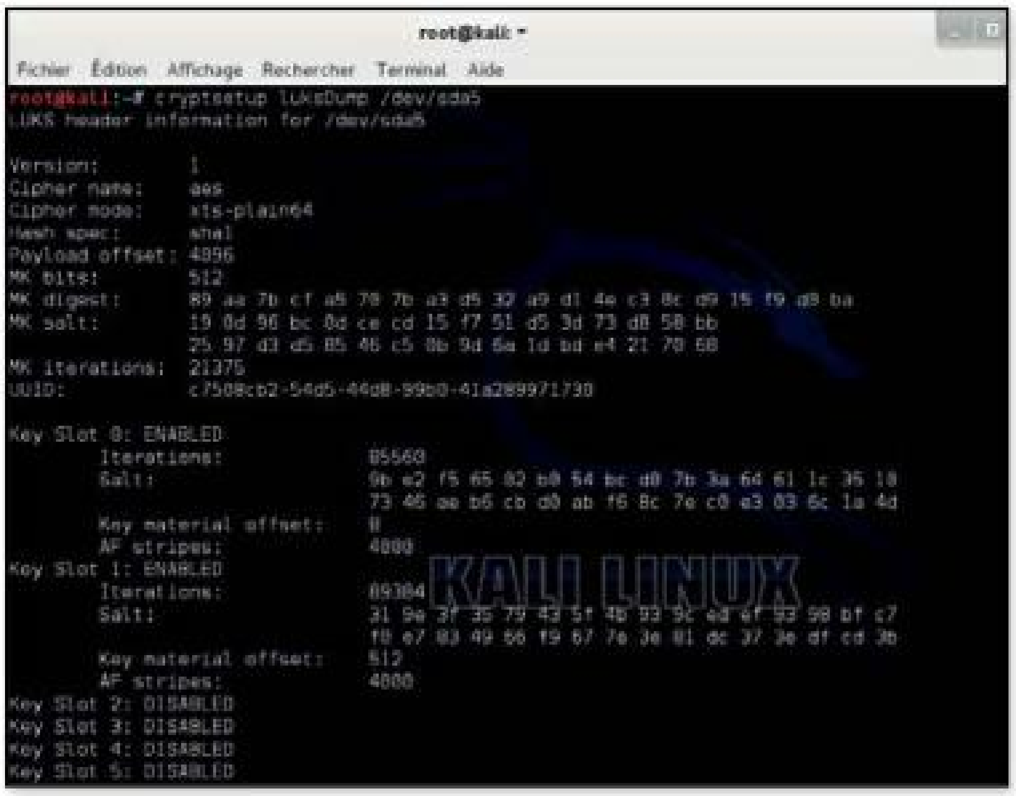
Refaites **root@kali:~# cryptsetup luksDump /dev/sda5** pour constater que les **Key Slot 0** et **1** sont en position **DISABLED**. C'est normal puisque la phrase secrète qui tue les a réinitialisés! Placez votre clé USB dans le PC et transférez le fichier



luksheader.back.enc dans **Computer/Home**.
Tapez **root@kali:~# openssl enc -d -aes-256-cbc -in luksheader.back.enc -out luksheader.back**
puis le mot de passe qui a servi à chiffrer le header (voir l'étape 3 du précédent pas à pas).

03 DUMP DU HEADER ET RÉCUPÉRATION DES DONNÉES

Tapez ensuite **root@kali:~# cryptsetup luksHeaderRestore --header-backup-file luksheader.back /dev/sda5** pour restaurer le header.
Tapez **YES** en capitale pour valider puis **root@kali:~# cryptsetup luksDump /dev/sda5** pour charger votre header tout neuf.
Vos **Key Slot 0** et **1** sont restaurés! Redémarrez le PC en prenant



soin de retirer le DVD et lorsque le système vous le demandera vous n'aurez qu'à taper votre première phrase secrète, celle qui donne accès aux données. Vous retrouverez votre interface avec tous vos fichiers!

DÉBUTANT ?

Vous débutez sous Kali Linux et vous souhaitez en savoir plus ? En suivant ce lien, vous trouverez une mine d'informations inestimables sur ce système. Apprenez comment installer correctement Linux avec les nouveaux BIOS UEFI, lancer une machine virtuelle, configurer un VPN, installer Tor, «tester» une clé WiFi, booter depuis un périphérique USB, etc.

Lien : **www.kali-linux.fr/tutoriels**

DÉTERMINER LE TYPE D'UN HASH

Depuis notre série d'articles sur le logiciel John The Ripper, nous recevons beaucoup de courrier de lecteurs concernant les hash et leurs différents types. Pour contenter tout le monde, nous allons faire le point dessus en essayant de déterminer le type d'un hash et en utilisant cette information pour gagner du temps lorsqu'il s'agira de retrouver le mot de passe correspondant.



LEXIQUE

***HASH :**
Les mots de passe ne sont jamais écrits en clair dans une base de données ou un ordinateur, ils sont codés avec une fonction de hachage. Il en existe plusieurs : MD5, SHA256, NTML, etc. Notez qu'un hash comme **721a9b52bfcea cc503c056e3b9b93cfa** ne correspond qu'à un seul mot de passe.

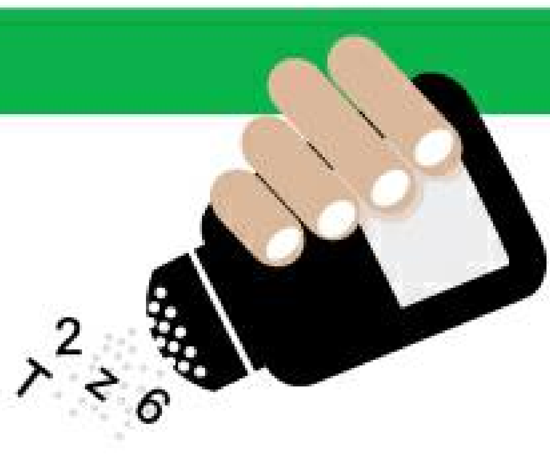
Dans nos précédents numéros nous avons abordé les attaques par dictionnaire et «brute force» à partir d'un hash pour retrouver le mot de passe correspondant. Or il est beaucoup plus rapide pour un logiciel de faire cette manœuvre si vous savez précisément quel type de hash est utilisé. Effectivement, au milieu de ces suites alphanumériques, il n'est pas facile de s'y retrouver d'autant qu'il en existe des dizaines ainsi que diverses techniques de «salage» (voir encadré). Pour cibler directement la recherche du mot de passe sur un type de hash précis, nous utiliserons le script Python HashTag. Ce dernier va reconnaître l'empreinte d'un hash pour vous désigner son type : MD5, SHA, MySQL, etc.

LE LANGAGE PYTHON À LA RESCOUSSE

Parfois HashTag ne trouvera pas précisément le type utilisé, mais vous donnera un panel de possibilité (car certains hash sont très proches au niveau de leurs structures). C'est largement suffisant pour gagner du temps et éliminer une bonne centaine de fonctions...

UN PEU DE SEL DANS VOTRE HASH ?

Le salage est une méthode permettant de renforcer la sécurité des mots de passe. Au lieu d'utiliser une méthode de hachage connue (MD5, etc.), on va y ajouter une valeur supplémentaire (une chaîne aléatoire) pour brouiller les pistes et éviter que le mot de passe n'ait qu'un seul hash équivalent.



0100110101000100010101011001001001010100010 0101001010010101010010000111010101010

Utilisation de HashTag.py

CE QU'IL VOUS FAUT

HASHTAG

OÙ LE TROUVER ? : **http://goo.gl/vQx8E9**

DIFFICULTÉ : ☠☠☠

01 INSTALLATION



Avant de commencer, il va falloir installer le langage Python sur votre machine. Préférez la version 2.7 et ne changez pas le répertoire d'installation par défaut. Téléchargez ensuite HashTag.py en suivant notre lien. En bas de la page, faites un clic droit dans le lien et faites **Enregistrer la cible du lien sous**. Placez-le ensuite dans le répertoire **C:\Python27**.

02 LA RECHERCHE

Avec tout ça, vous êtes prêt ! Faites **Maj + clic droit** dans le répertoire **C:\Python27** et choisissez **Ouvrir une fenêtre de commandes ici**. Il faudra alors taper **python hashtag.py -sh [votre hash]**. Lors de notre premier essai, nous n'avons pas eu de chance, car le hash choisi pouvait potentiellement être d'une vingtaine de types différents. Dans ce cas, il vaudra mieux commencer la recherche par les plus fréquents. Notre deuxième essai a été plus concluant puisqu'en excluant les variantes, HashTag nous a permis de réduire le champ de recherche à 4 types de hash différents ! Nous savons ici que cette suite alphanumérique a de grandes chances d'être un SHA-512. Si vous utilisez le logiciel Hashcat au lieu de John the Ripper, HashTag vous donnera le mode de recherche correspondant...



03 AVEC JOHN THE RIPPER



Lorsque vous savez à quel type de hash vous avez à faire, vous allez gagner beaucoup plus de temps avec John the Ripper ! Par exemple, lorsque vous êtes sûr qu'il s'agit d'un MD5 il faudra taper
john -format:raw-md5 hash.txt
ou
john -format:raw-sha512 hash.txt s'il s'agit d'un SHA-512.
En sachant où regarder, il n'a fallu que 16 secondes à John the Ripper pour trouver le mot de passe azerty alors qu'il aurait de nombreuses minutes en essayant tous les types de hash (le logiciel ne peut cracker différents types en même temps). Si HashTag vous donne plusieurs types de hash possible, il faudra les essayer un à un. Pour les hash salés, c'est un peu plus compliqué, car il faudra alors créer une fonction de hachage dynamique...



SUR NOTRE CD

Sur notre CD, retrouvez notre série d'articles sur John the Ripper, un puissant logiciel permettant de récupérer un mot de passe à partir d'un hash



PARTAGEZ DES FICHIERS INCOGNITO

Vous utilisez Tor ? Un peu, beaucoup, à la folie ? Pour vous, nous avons trouvé la solution idéale pour partager des fichiers en utilisant ce protocole. Avec son interface graphique simple, OnionShare va vous permettre de faire passer des documents sensibles (ou pas !) à vos proches et amis. Les services secrets et autres petits curieux n'y verront que du feu...

SUR NOTRE CD

Sur notre CD, retrouvez les articles sur Tor et Bitmessage que nous avons réalisé dans nos derniers numéros...

LEXIQUE

TOR : Tor est un réseau informatique décentralisé qui utilise une architecture «en oignon» (d'où le logo). Le système est composé de routeurs organisés en couches. Les paquets de données transitent d'un routeur vers un autre en laissant peu de traces sur leur origine.

Dans notre précédent numéro, nous vous avons parlé de Tor, ce protocole permettant de surfer sans trahir son identité ou sa localisation. Nous vous avions aussi parlé de Bitmessage dans notre numéro 18. Ce logiciel, basé sur Tor, permet quant à lui de communiquer avec d'autres correspondants. Il ne restait alors qu'à trouver un moyen de transférer des fichiers en utilisant Tor. Pour cela, il existe OnionShare, un petit script python qui va créer un serveur temporaire sur votre ordinateur. OnionShare va générer une URL en .onion uniquement accessible via Tor.

UNE CLÉ UNIQUE ET UN TRANSFERT ANONYME

La sécurité est de mise puisqu'en plus de cette URL, le logiciel va aussi lui adjoindre une clé unique qui servira à authentifier votre correspondant. Il faudra juste que votre machine reste allumée le temps du transfert. Il est même possible de fermer le serveur lorsque les fichiers seront transférés. Cerise sur le gâteau, votre correspondant n'aura même pas à installer OnionShare pour réceptionner les fichiers puisqu'une simple connexion à Tor suffit pour accéder à l'URL de votre service caché. Surf, messagerie et partage de fichier : nous avons fait le tour des possibilités avec le logiciel Tor !

N'ENCOMBREZ PAS TOR !

Attention, pour éviter d'encombrer Tor, n'utilisez pas OnionShare comme un système de partage de films ou de musiques. Le but du logiciel est de partager des fichiers potentiellement «sensibles» vers ou en direction de pays où la surveillance des citoyens est maximale. Pour le partage de gros volume ou de contenu multimédia, il existe RetroShare par exemple...



Première utilisation de OnionShare

CE QU'IL VOUS FAUT

ONIONSHARE
OÙ LE TROUVER ? : **https://onionshare.org**

TOR
OÙ LE TROUVER ? : **www.torproject.org**

DIFFICULTÉ :

01 PRÉ-REQUIS

Pour envoyer des fichiers avec OnionShare, il faudra que vous ayez Tor installé sur votre PC. Pour la réception, vos correspondants n'auront pas besoin de OnionShare, mais Tor reste obligatoire. Téléchargez la dernière version du Tor Browser et paramétrez-la (regardez notre article à ce sujet sur notre CD si vous êtes perdu).



02 L'INTERFACE

Il faudra ensuite installer OnionShare. Aucune difficulté, ici, vous n'êtes même pas obligé d'installer Python pour faire fonctionner l'application. Une fenêtre devrait s'afficher avec un espace pour glisser-déposer des fichiers, des boutons pour ajouter des éléments et une case à cocher si vous voulez arrêter le serveur automatiquement. Cette dernière est utile si vous souhaitez arrêter le partage lorsque votre correspondant aura récupéré les fichiers.





03 VOTRE SERVEUR «MAISON»

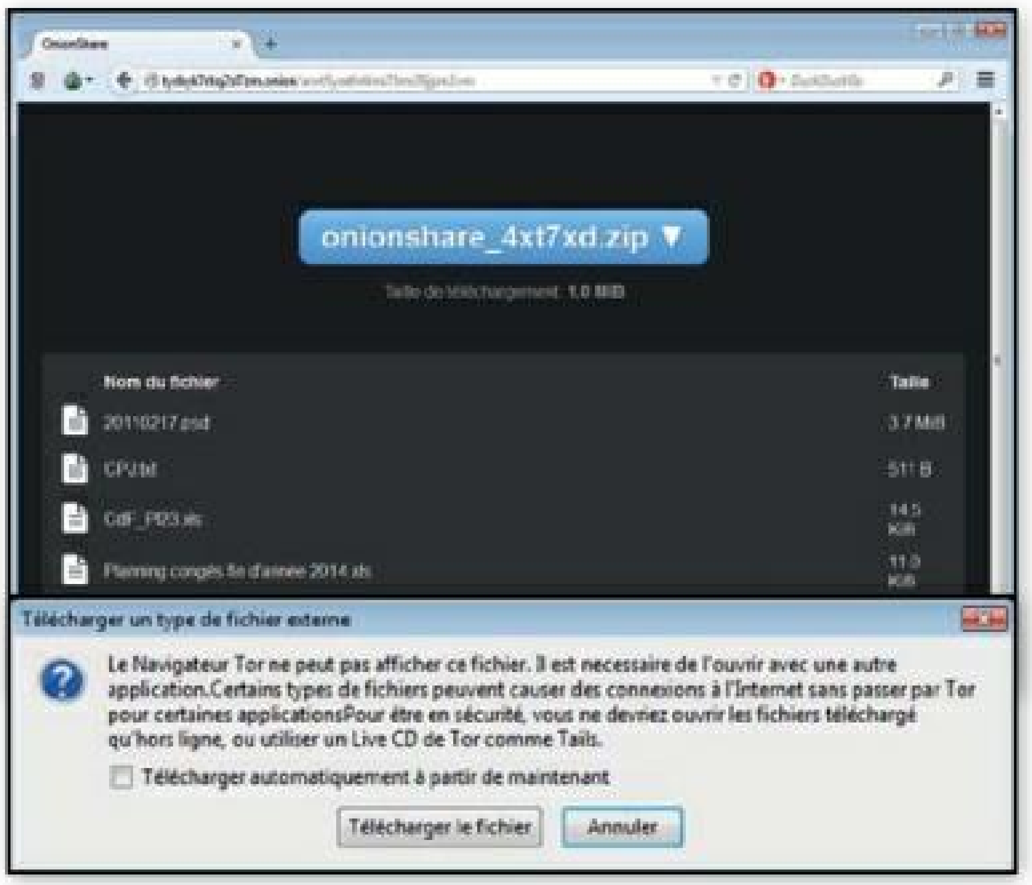
Mettez autant de fichiers et dossiers que vous voulez et cliquez sur **Démarrer le serveur**. Attention, il faudra que Tor soit connecté à Internet pour que la magie opère. OnionShare va alors simplement générer un lien qui dirigera sur un service caché (hidden service), une page Internet accessible uniquement aux utilisateurs de Tor. À tous les utilisateurs ? Non ! Seulement à celui de votre choix. En effet, après l'URL en **.onion** caractéristique des services cachés, une clé de chiffrement est ajoutée (vous pouvez d'ailleurs l'envoyer à part) !





04 LA RÉCEPTION

Envoyez ce lien à votre ami par un moyen sécurisé (une messagerie comme Bitmessage par exemple) si le contenu est sensible. Armé de Tor, votre petit camarade n'aura qu'à cliquer pour récupérer les fichiers/dossiers regroupés en un seul ZIP. Une fois que le transfert sera terminé, le serveur qui aura été créé sur votre machine va automatiquement s'arrêter si vous avez cliqué sur la case idoine. Notez que pour ne pas trahir son IP, votre correspondant devra ouvrir vos fichiers hors ligne ou utiliser le Live CD Tails compatible avec Tor...



LUCKY PATCHER : NE (RE)PAYEZ PLUS VOS APPLIS



LEXIQUE

***PATCH :** Correctif utilisé sur une application pour la modifier. Ici il ne s'agit pas d'améliorer des applis mais d'éviter qu'elles n'aillent vérifier que vous êtes bien titulaire d'une licence...

***ROOT :** Il s'agit avant tout d'une manipulation permettant d'avoir le contrôle total sur votre appareil, le mode SuperUser : installation d'appli proposant des fonctionnalités inédites, personnalisation de l'interface, «tweak» en tous genres, etc.

Soyons clairs, Lucky Patcher est une application qui ouvre la voie au piratage. Il s'agit en fait de contourner la vérification de la licence d'une appli ou d'un jeu. Nous préférons voir cette méthode comme un moyen de récupérer des droits sur une application que vous auriez déjà payée par exemple ou de permettre de tester plus sérieusement une appli très chère...

Le système Android fonctionne avec des fichiers APK qui viennent s'installer sur votre smartphone ou tablette un peu comme un EXE vient s'installer sur Windows. Mais là où on vous demandera une clé de licence sur PC, Google enregistre votre achat et vous transfère une licence numériquement signée que vous seule pouvez utiliser sur votre machine. Lorsque vous perdez votre téléphone par exemple, Google vous donne l'occasion de télécharger une nouvelle fois vos applis avec les licences, mais imaginez que vous perdiez aussi vos identifiants... Dans ce cas vous perdez votre compte et vos précieux achats.

CONTOURNER LES VÉRIFICATIONS DE LICENCE

Lucky Patcher va simplement contourner la vérification des licences sur votre machine pour lancer les applis que vous avez déjà achetées. Bien sûr cette méthode permet aussi à des petits malins de lancer des applications qu'ils n'ont jamais payées. Mais après tout, pourquoi ne pas utiliser Lucky Patcher pour tester la version complète d'une appli avant de dépenser son argent ? Les versions démos sont souvent bridées et il est parfois difficile de se faire un avis définitif avec une version limitée... Notons aussi que Lucky Patcher peut très bien supprimer les publicités des applications gratuites ou geler des applis trop gourmandes. Attention, l'appli ne fonctionne que sur les appareils «rootés».

PAS À PAS

Contournement de licence

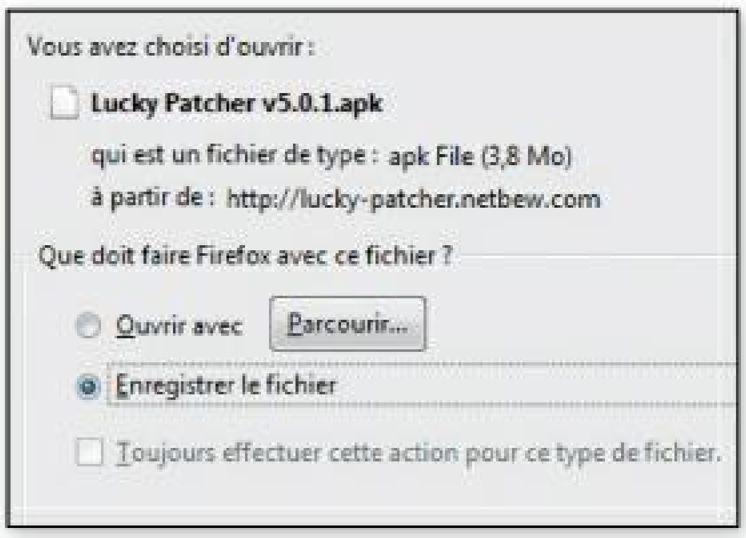
CE QU'IL VOUS FAUT

LUCKY PATCHER

OÙ LE TROUVER ? : **http://lucky-patcher.netbew.com**

DIFFICULTÉ :

01 PRÉ-REQUIS



Téléchargez et installez Lucky Patcher sur votre appareil rooté (avec la Busy Box d'installée). Sur le Net vous trouverez des applications aux formats APK avec des dossiers de licence qui commence par com. Il faudra suivre les instructions contenues dans le fichier texte, mais la plupart du temps le procédé sera le même.

02 LES OPTIONS

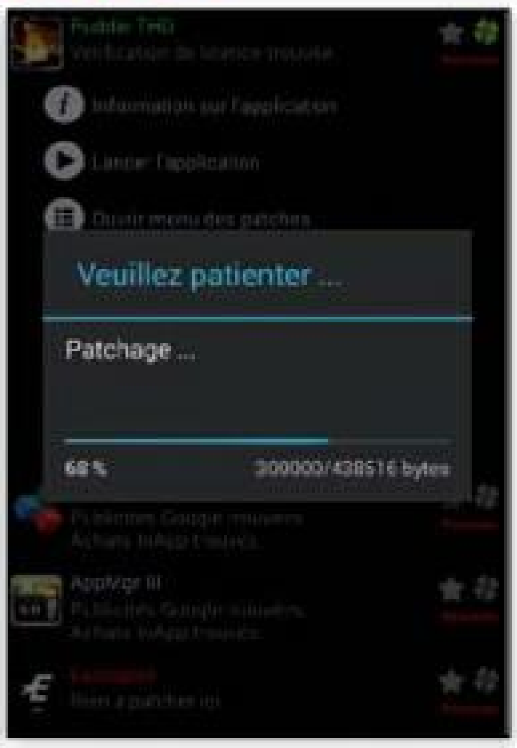




Installez l'APK de l'application que vous convoitez, mais surtout ne la démarrez pas. Dans notre cas nous essaierons d'installer le jeu Puddle. Sans Lucky Patcher, le jeu refusera de démarrer, car la licence n'est pas valide. Lancez Lucky Patcher et faites un appui long sur Puddle. Dans la liste des actions, vous pourrez notamment **Supprimer les publicités, Créer un .apk modifié** (pour intégrer un patch directement à l'APK) ou geler une application qui pomperait trop de ressource.

03 SUPPRESSION DE LA VÉRIFICATION



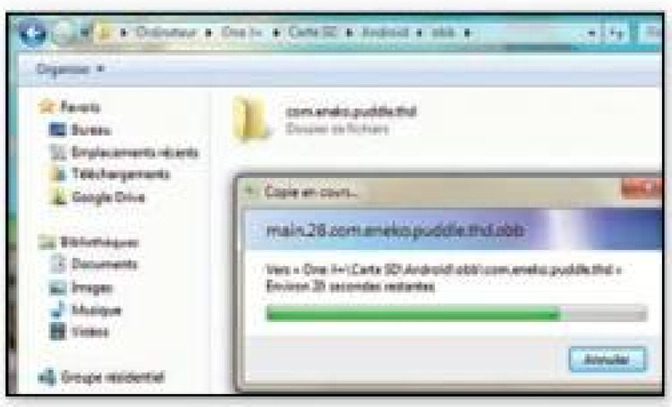


Mais ce qui nous intéresse ici c'est **Supprimer la vérification de licence**. Utilisez le mode **Auto** et attendez que Lucky Patcher aille chercher le patch adéquat (il vous faudra une connexion à Internet durant cette étape). A la fin, l'appli vous donnera une approximation de la réussite de la manipulation. Dans notre cas, Puddle avait 42 % de chance de se lancer.

04 LANCEZ VOTRE APPLI



Selon l'appli que vous voulez faire fonctionner, il vous sera aussi demandé de copier à la main les dossiers d'une licence (qui fera office de «carte blanche»). Copiez le dossier dans **/sdcard/Android/Obb** et lancez enfin votre application. Dans notre cas, et même avec seulement 42 % de chance, le jeu se lance. Notez qu'il s'agit de la version complète !



Lucky Patcher ne fonctionne pas avec votre fichier APK ? Pas de panique, les développeurs ajoutent des patchs tous les jours !

UN NETTOYEUR DE CLÉS USB

Marre des clés USB de mamy pleines de virus ou de celles des collègues qui ont traîné on ne sait où ? Avant de brancher n'importe quel périphérique dans votre ordinateur pourquoi ne pas vérifier qu'ils sont sécurisés ? Notre système à base de Raspberry Pi permet même de récupérer les fichiers vérolés...

SUR NOTRE CD

Si vous avez raté les derniers numéros de *Pirate Informatique*, retrouvez tous les précédents articles concernant le Raspberry Pi sur notre CD : la présentation de l'appareil, la conception d'un Media Center, d'un système de vidéosurveillance, d'une borne d'arcade, d'un récepteur Webradio, d'une radio FM amateur et d'un Cloud personnel.



Nous connaissons tous ce problème. Untel vient chez vous avec une clé USB ou un disque dur externe et vous demande de le brancher sur votre PC pour vous donner ou montrer des documents. Rien de bien sorcier mais une question vous taraude : Où diable cette clé a-t-elle bien pu se retrouver avant ? D'une main tremblante, vous connectez le périphérique de stockage sur votre machine en priant que votre antivirus ne vous lâche pas...

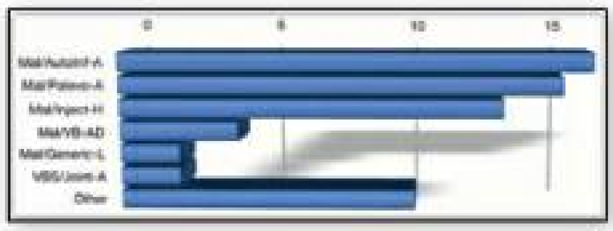
DES FICHIERS CONVERTIS VERS DES FORMATS MOINS DANGEREUX

Car bien sûr, vous avez un antivirus à jour mais pourquoi prendre le moindre risque ? Avec un Raspberry Pi et la distribution gratuite CIRCLean, vous pourrez vous confectionner un «nettoyeur». Mettez la clé louche dans le port du haut et une clé saine dans celui du bas. CIRCLean va transférer les documents dans des formats moins dangereux (les PDF seront transformés en HTML, etc.) et va enrayer les vers, virus, etc. Il suffit de relier le Raspberry Pi à l'alimentation (celle d'un smartphone en Micro-USB fera l'affaire).
Vous pouvez brancher un écran pour voir ce qui se passe mais ce n'est pas une obligation puisque vous saurez que l'opération est terminée lorsque les petites LED vertes de la carte s'arrêteront de clignoter...

LEXIQUE

***RASPBERRY PI :**
Le Raspberry Pi est un micro-ordinateur (ou nano-ordinateur) créé dans le but d'encourager l'apprentissage de l'informatique aux personnes avec peu de moyens ou dans les pays en voie de développement. Tous les composants sont réunis sur une seule carte et le tout est livré sans moniteur, clavier, souris, système d'exploitation, disque dur ou alimentation pour privilégier la récupération et les licences libres.

UNE VACCINATION ?



Notre solution avec CIRCLean sert plus à «assainir» le contenu d'une clé qu'à la désinfecter. Pour cela, il existe des solutions antivirus comme USB Disk Security ou AutoRun Antivirus Pro. Ce dernier va «vacciner» une clé ou un disque dur externe pour éviter les attaques «autorun» (des malwares qui infecteraient automatiquement le système dès le branchement du périphérique). Choisissez le disque dur ou la partition à vacciner puis cliquez sur **Vaccine** pour protéger votre système. Cochez la case **AutoVaccine new plugged devices at logon** pour vous protéger des appareils qui seraient branchés en votre absence.

Lien : **http://goo.gl/Djr9h**

CIRCLean sur votre Raspberry Pi

CE QU'IL VOUS FAUT

CIRCLEAN
OÙ LE TROUVER ? : **http://circl.lu/projects/CIRCLean**

WIN32 DISK IMAGER
OÙ LE TROUVER ? : **http://sourceforge.net/projects/win32diskimager**

Un Raspberry Pi ; Un câble Micro-USB (pour l'alimentation du Raspberry Pi) Une carte SD d'au moins 8 Go ; Une clé USB de plus grande capacité que celle que vous voulez désinfecter

DIFFICULTÉ :

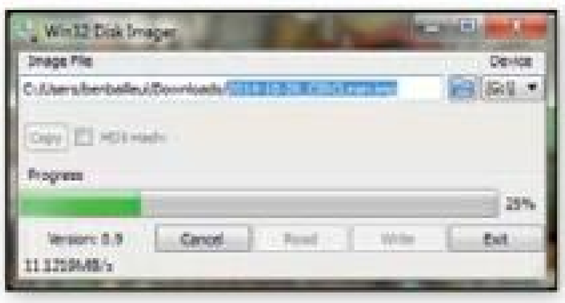
01 TÉLÉCHARGEMENT DE CIRCLEAN

Commençons par placer l'image de CIRCLean dans la carte SD. Sur le site, téléchargez la dernière version de l'image puis dézippez-la (utilisez 7-Zip si vous n'avez pas de logiciel pour le format GZ). Pour mettre le contenu du fichier IMG dans la carte, un simple copier-coller ne suffit pas, il faudra utiliser le logiciel Win32 Disk Imager. Téléchargez-le en suivant notre lien et munissez-vous d'une carte SD d'au moins 8Go.



02 INSTALLATION DES FICHIERS

Lancez Win32 Disk Imager, sélectionner **2014-10-26_CIRCLean.img** avec l'icône en forme de dossier puis spécifiez l'emplacement de la carte SD dans la colonne **Device**. Ne vous trompez pas sous peine d'effacer le contenu d'un de vos disques durs! Faites **Write** et attendez la fin du processus. Notez que pour revenir en arrière et récupérer une carte en FAT32, il faudra passer par le logiciel gratuit MiniTool Partition Wizard.



03 AU TRAVAIL !

Connectez la carte SD puis branchez la clé USB suspecte dans le port du haut et celle qui servira à récupérer les données en bas. Il ne vous reste plus qu'à connecter l'alimentation du Raspberry Pi. Après la mise en route (LED rouge), vous verrez la LED verte s'allumer. Si celle-ci ne fonctionne plus ou si votre modèle de Raspberry Pi n'en comporte pas, branchez un casque audio sur le port jack. Tant que vous entendrez la musique, le processus n'est pas encore terminé.



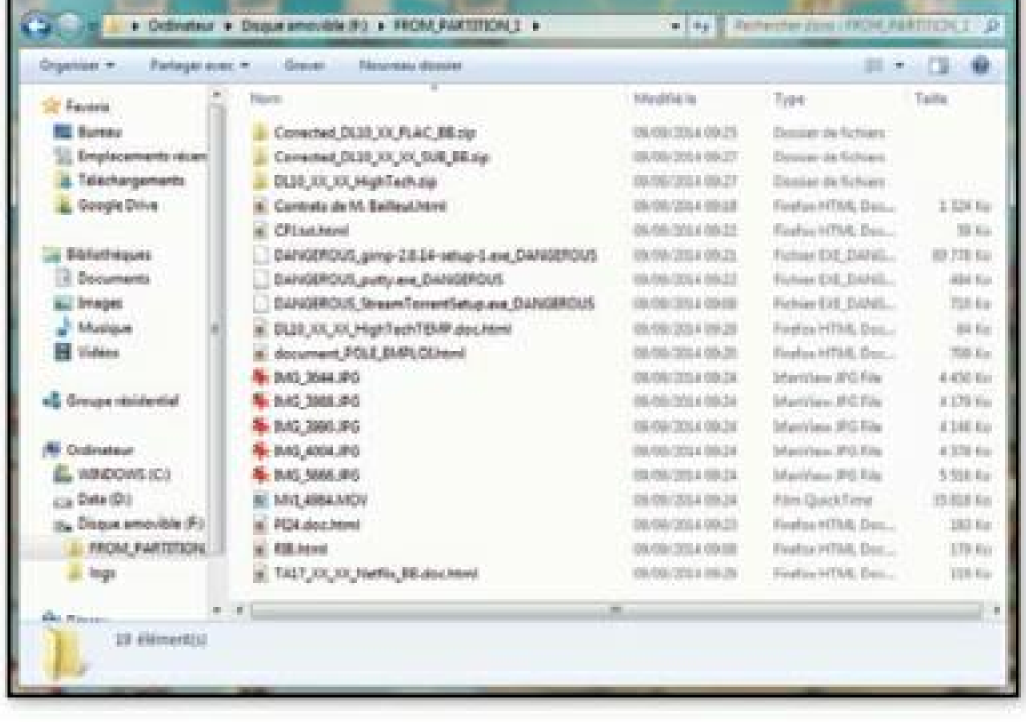
04 CONVERSION DES FICHIERS

Pour «voir» les étapes, vous pouvez aussi brancher le Raspberry sur un écran ou un téléviseur via le port HDMI. Une fois terminé, débranchez l'alimentation et placez la clé USB saine dans votre PC. Vous y trouverez un dossier logs contenant les journaux des activités de CIRCLean ainsi qu'un répertoire FROM_PARTITION_1. Vous verrez que certains formats de fichier particulièrement porteur de malwares ont été convertis: les PDF et les DOC notamment. Vous pourrez tout de même lire leur contenu.



05 LE CAS DES EXE

Libre à vous de les convertir à nouveau vers le format de votre choix. Notez aussi que les fichiers EXE sont systématiquement neutralisés par l'ajout de la mention DANGEROUS dans l'extension. Dommage qu'un véritable antivirus ne soit pas présent dans la distribution car avec cette méthode, aucun EXE ne trouvera grâce aux yeux de CIRCLean... Bien sûr, vous pourrez renommer votre exécutable pour le rendre «utilisable» si vous êtes sûr de son intégrité.

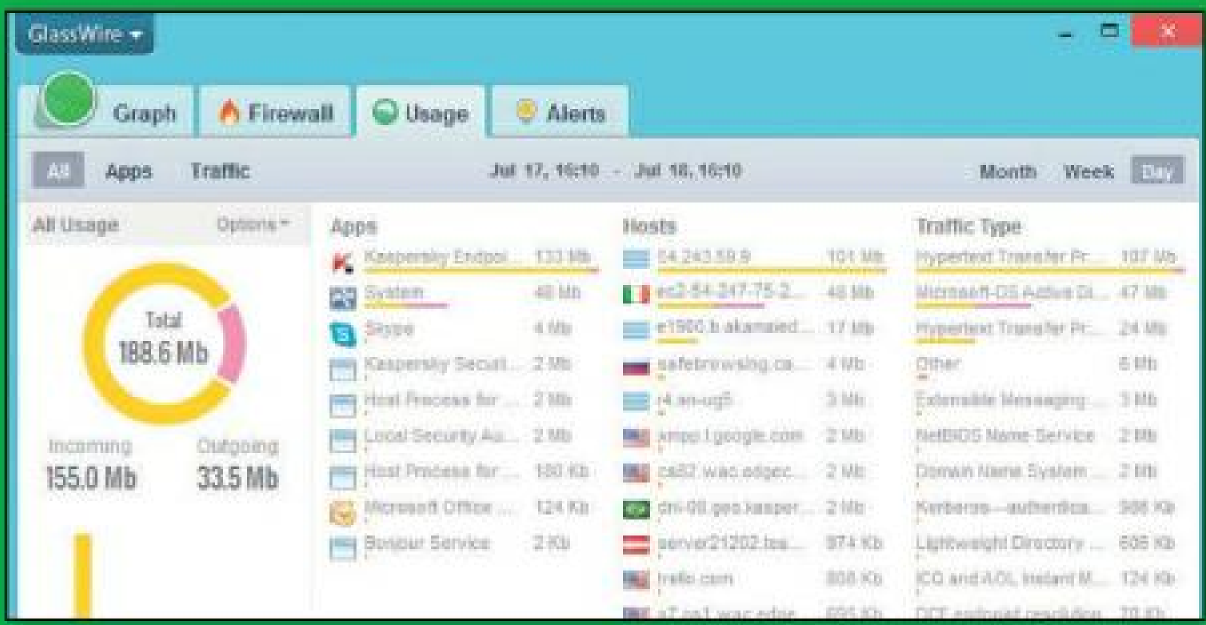


#1 Surveillez votre réseau

AVEC GLASSWIRE

Le logiciel GlassWire permet de surveiller l'activité sur votre réseau. Là où les autres programmes de ce type rivalisent d'austérité, GlassWire est très agréable à l'œil et bien conçu. Vous pourrez garder un œil sur l'utilisation de votre bande passante (quel processus consomme le plus de données, etc.) mais aussi sur l'utilisation des ports. Le logiciel intègre aussi un module de détection de modifications de fichiers et déjoue les attaques «ARP poisoning». Idéal pour trouver les activités louches ou les programmes un peu trop «bavards»...

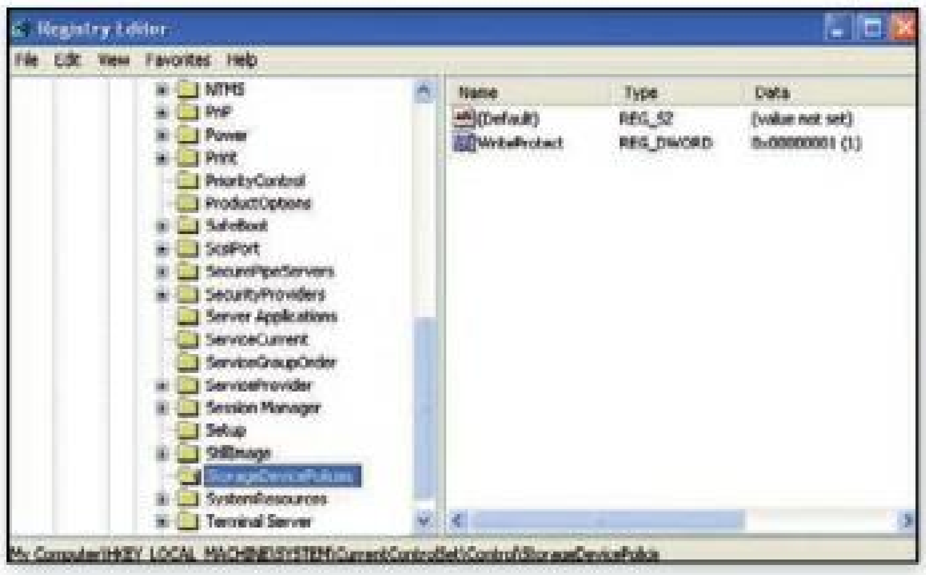
Lien: **www.glasswire.com**



#2 Formater une clé protégée en écriture

AVEC WINDOWS 7 & 8

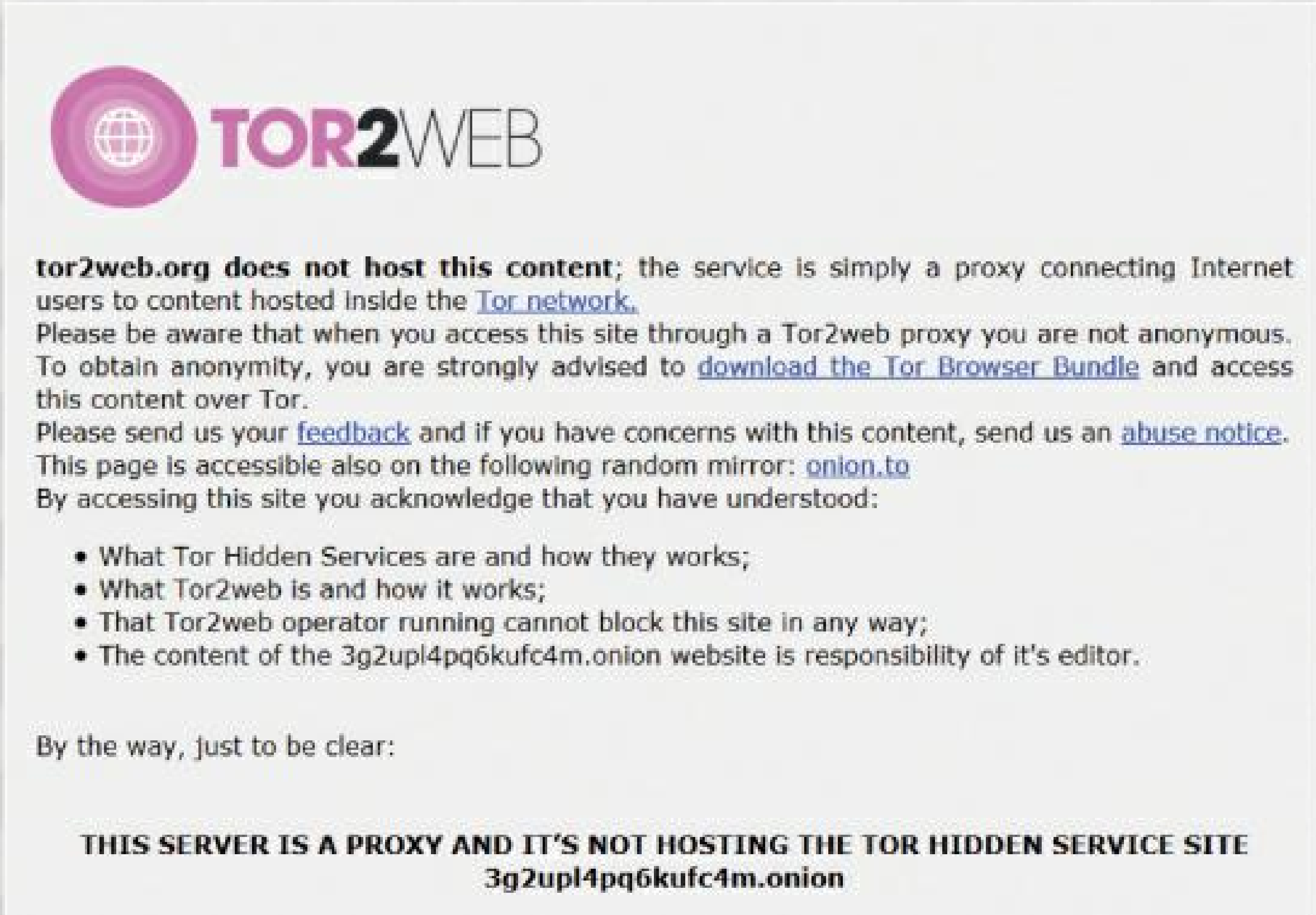
Lorsque vous tentez d'ouvrir une clé USB, Windows vous prévient que cette dernière est protégée en écriture ? Impossible d'avoir accès aux fichiers et encore moins d'en effacer le contenu. Pas de problème pourtant, il suffit de passer par le registre de Windows. Appuyez en même temps sur la **touche Windows** et **R**. Dans le champ qui s'affiche, tapez **regedit** et validez. Trouvez la clé suivante : **HKEY_LOCAL_MACHINE \SYSTEM\ CurrentControlSet\Control\StorageDevicePolicies**. Changez la valeur de **Writeprotect** en **0**.



#3 Accédez aux sites Tor... sans Tor

AVEC TOR2WEB ET ONION.TO

Si vous connaissez Tor, vous savez que ce logiciel permet de protéger votre anonymat lorsque vous surfez sur Internet mais qu'il permet aussi d'accéder à des sites cachés, les fameux «hidden services». Si vous n'avez ni l'envie ni la patience d'installer Tor mais que vous désirez tout de même accéder à un de ces sites en .onion, vous pouvez toujours le faire en passant par les proxy Tor2Web ou Onion.to. Il suffit pour cela de prendre l'URL d'un hidden service (comme celui-ci : **http://3g2upl4pq6kufc4m.onion**) et d'intégrer la clé comme cela : **https://3g2upl4pq6kufc4m.tor2web.org**. Vous devrez ensuite cliquer sur **I agree with the terms, let me access the content**. Attention ces deux sites ne protégeront ni votre IP ni votre activité. Pour l'anonymat, il faudra absolument passer par Tor. Sans clé, le lien **https://tor2web.org** ne vous mènera nulle part. Voici donc une liste de sites cachés : **http://goo.gl/Nx6oiA**.



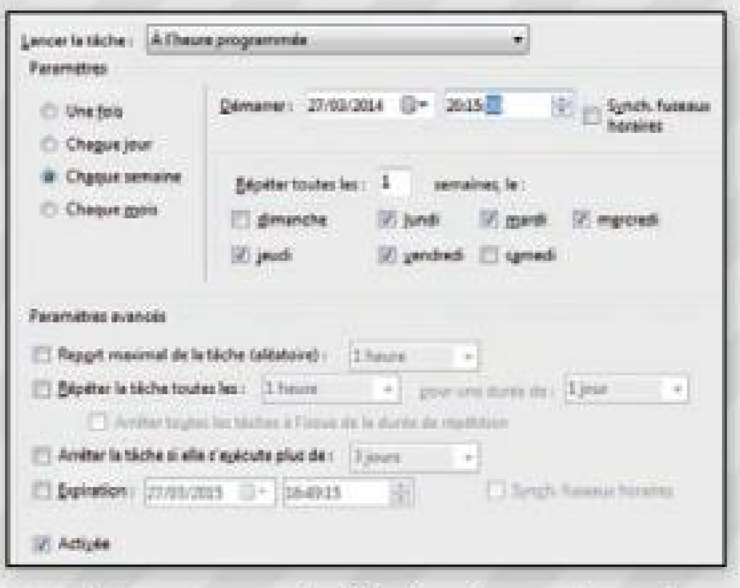
Lien : **https://tor2web.org**

Lien : **https://onion.to**

#4 Éteindre votre ordinateur à une heure précise

AVEC WINDOWS 7 ET 8

Le planificateur de tâches de Windows permet de paramétrer tout un tas de choses, mais vous pouvez aussi programmer l'extinction de votre PC. Ouvrez le volet de recherche accessible depuis la Charms Bar (la barre de droite) et entrez le terme **tâches** dans les **Paramètres**. Pour Windows 7, tapez juste tâches dans le champ de recherche du menu **Démarrer**. Cliquez sur **Planificateur de tâches** et dans le volet droit, sélectionnez **Créer une tâche**. Donnez un nom à cette dernière et cochez la case **Exécuter avec les autorisations maximales**. Ouvrez ensuite l'onglet **Déclencheurs** et faites **Nouveau**. Choisissez alors la fréquence de la tâche en sélectionnant l'option **Chaque semaine** par exemple. Cochez la case devant les jours de la semaine où l'arrêt automatique sera effectué et choisissez l'heure de l'extinction de votre PC. Cliquez sur **OK** puis ouvrez l'onglet **Actions**. Faites encore une fois **Nouveau** et tapez la commande **shutdown** dans le champ **Program/script**. Tapez le paramètre **/S** dans le champ **Ajouter des arguments** et cliquez sur **OK**.



#5 Un appareil pour le pentesting

AVEC KALI LINUX POUR ANDROID

Plus la peine de présenter Kali Linux (anciennement BackTrack), la distribution Linux spécialisée dans la sécurité informatique et l'audit réseau. La bonne nouvelle c'est que les heureux possesseurs d'appareils Nexus (4, 5, 7 et 10) peuvent maintenant s'adonner au plaisir du pentesting avec NetHunter. Ce système de substitution permet d'utiliser votre appareil Android comme une carte Wi-Fi supportant les injections (DPI) mais aussi d'utiliser toutes les capacités de Kali Linux en «stand-alone» : autodestruction de donnée, prise de contrôle à distance, attaque HID, BadUSB, etc. On attend de pied ferme que d'autres appareils viennent s'ajouter à la liste de compatibilité !

Lien: **http://nethunter.com**

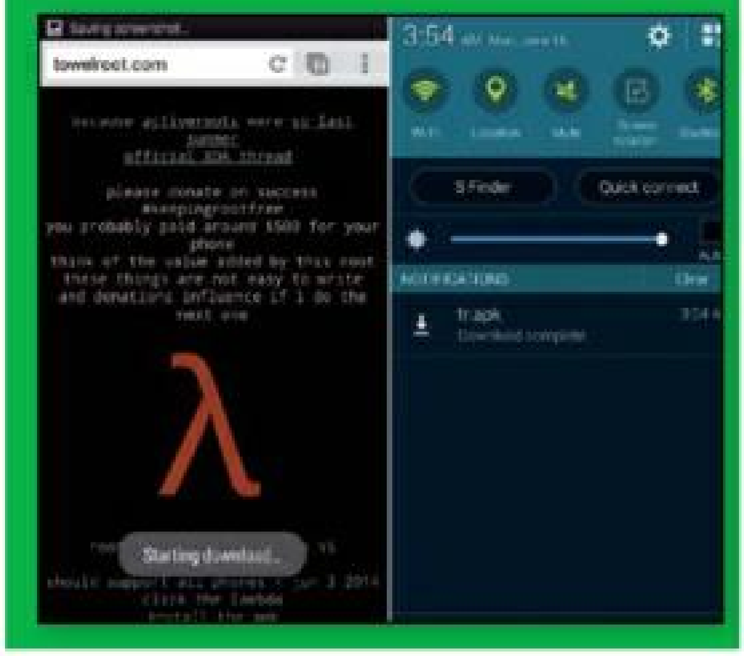


#7 Rooter son smartphone

AVEC TOWELROOT

Il n'est pas toujours facile de rooter son smartphone : tutos peu clairs, différence de protocole entre les mêmes versions d'appareil, etc. Heureusement voici Towelroot, une application créée par GeoHot (un hacker à l'origine de plusieurs prouesses) permettant de rooter n'importe quel téléphone sans effort. Il s'agit d'une simple appli au format APK que vous devrez lancer sur votre smartphone ou votre tablette. Il suffit de s'assurer que votre téléphone autorise les applications de source inconnue (**Paramètres > Sécurité > Sources Inconnues**). Attention, comme Towelroot exploite une faille du noyau Linux d'Android, cette dernière risque d'être comblée par les fabricants. Enfin quand on connaît la rapidité légendaire de LG, HTC, Sony et de leurs petits copains...

Lien : **https://towelroot.com**





NOUVEAU !

INSCRIVEZ-VOUS GRATUITEMENT !

La mailing-list officielle de **Pirate Informatique**

De nombreux lecteurs nous demandent chaque jour s'il est possible de s'abonner. La réponse est non et ce n'est malheureusement pas de notre faute. En effet, notre magazine respecte la loi, traite d'informations liées au monde du hacking au sens premier, celui qui est synonyme d'innovation, de créativité et de liberté. Depuis les débuts de l'ère informatique, les hackers sont en première ligne pour faire avancer notre réflexion, nos standards et nos usages quotidiens.

Mais cela n'a pas empêché notre administration de référence, la «Commission paritaire des publications et agences de presse» (CPPAP) de refuser nos demandes d'inscription sur ses registres. En bref, l'administration considère que ce que nous écrivons n'intéresse personne et ne traite pas de sujets méritant débat et pédagogie auprès du grand public. Entre autres conséquences pour la vie de nos magazines : pas d'abonnements possibles, car nous ne pouvons pas bénéficier des tarifs presse de la Poste. Sans ce tarif spécial, nous serions obligés de faire payer les abonnés plus cher ! Le monde à l'envers...

La seule solution que nous avons trouvée est de proposer à nos lecteurs de s'abonner à une mailing-list pour les prévenir de la sortie de nos publications. Il s'agit juste d'un e-mail envoyé à tous ceux intéressés par notre magazine et qui ne veulent le rater sous aucun prétexte.

Pour en profiter, il suffit de s'abonner directement sur ce site

http://eepurl.com/FlOOD

(le L de «FlOOD» est en minuscule)

ou de scanner ce QR Code avec votre smartphone...

TROIS BONNES RAISONS DE S'INSCRIRE :

1 Soyez averti de la sortie de *Pirate Informatique* en kiosques. Ne ratez plus un numéro !

2 Vous ne recevrez qu'un seul e-mail par mois pour vous prévenir des dates de parutions et de l'avancement du magazine.

3 Votre adresse e-mail reste confidentielle et vous pouvez vous désabonner très facilement. Notre crédibilité est en jeu.

Votre marchand de journaux n'a pas *Pirate Informatique* ?

L'autre problème de taille pour nos lecteurs est la difficulté à trouver Pirate Informatique. Si votre marchand de journaux n'a pas le magazine en kiosque, il suffit de lui demander (gentiment) de vous commander l'exemplaire auprès de son dépositaire ! Pour cela, munissez-vous du numéro de codification L12730. Ainsi vous n'aurez pas à faire tous les kiosques de votre ville pour le trouver !

LES SOUS-TITRES DANS TOUS LEURS ÉTATS



Fans de films en VO ou simplement impatients de regarder le dernier épisode de votre série préférée ? Même si vous êtes à l'aise avec les langues étrangères, les sous-titres sont la solution idéale lorsqu'il s'agit de ne perdre aucune miette des dialogues. Selon vos habitudes et votre matériel, voyons comment toujours avoir le sous-titre qu'il vous faut sous la main...

Les sous-titres que vous pouvez trouver sur le Net sont soit des captures de caractères récupérés sur des DVD ou des Blu-ray, soit des fichiers spécialement créés par des équipes de fans appelés fansubbers. Dans les deux cas, il s'agit de fichiers textes qui doivent être lus par votre logiciel de lecture en même temps que la vidéo. Tous les lecteurs vidéo prennent en charge les sous-titres : VLC, Windows Media Player, SPlayer, Media Player Classic, etc. Longtemps la méthode pour profiter d'une traduction a été de rechercher à la main sur Google le bon fichier (avec les approximations et décalages liés au framerate, aux différentes versions du film, etc.) puis de le renommer de la même manière que le fichier vidéo. Les choses ont évolué et il n'est désormais plus obligatoire de faire une recherche spécifique ou de garder dans le disque dur 15 versions de votre sous-titre pour espérer en avoir une de bonne. La plupart des solutions que nous vous proposons fonctionnent de la même manière : à chaque fois les logiciels iront chercher les sous-titres sur des bases de données distantes comme **www.opensubtitles.org/fr.**

SUR PC

Sur PC, la lumière est venue de VLSub. Nous savons que VLC Media Player est très à l'aise avec les sous-titres. Pourtant, nous avons trouvé une extension qui améliore encore plus la prise en charge de ces derniers. Après avoir installé VLSub, vous pourrez automatiquement récupérer les sous-titres du film que vous êtes en train de lire depuis OpenSubtitles. Plus besoin d'utiliser un logiciel séparé ou d'aller sur le site ! Tous les

INCRUSTÉ OU ENCAPSULÉ ?

Votre appareil ne supporte pas les sous-titres? Sachez qu'il est tout de même possible d'en profiter en incrustant les textes dans votre vidéo. Ils ne pourront plus être séparés, mais au moins n'importe quel lecteur pourra les afficher. Dans le logiciel Format Factory, choisissez votre format (tout type vers AVI par exemple) et dans les **Paramètres de sortie**, allez dans **Sous-titres additionnels** pour les implémenter avant de lancer votre encodage. Si vous aimez le MKV, il est aussi possible d'encapsuler une piste de sous-titres avec le logiciel MKVToolNix.

Lien: **www.pcfreetime.com/fr**
Lien: **www.bunkus.org/videotools/mkvtoolnix**



sous-titres disponibles pour un même film ou épisode sont affichés. Il suffit d'en choisir et de passer au suivant si ce dernier ne convient pas (voir notre prise en main).

SUR SMARTPHONE ET TABLETTE

Pour les appareils Android, l'application GMT Subtitles va scanner les fichiers multimédias présents sur votre machine et vous proposer des sous-titres adéquats. Gratuite, entièrement en français, l'application a le bon goût de ne pas contenir de publicités. Les fichiers seront placés «à côté» de votre vidéo pour lancer les deux avec votre lecteur préféré : MX Video Player, mVideoPlayer, MoboPlayer, VLC, etc. Pour les iPhone/iPad c'est un peu plus compliqué (comme toujours avec ces systèmes fermés !). Il faudra d'abord installer un lecteur compatible avec les formats de vidéos et de sous-titres les plus courants (par défaut, l'iPad ne lit en effet que les fichiers MP4). Ensuite, il faudra se tourner vers l'appli SubtitleFinder, disponible sur iTunes pour 0,89 €. Son fonctionnement est un peu différent : l'application va chercher, renommer et placer les sous-titres des vidéos présentes sur votre box ou lecteur de salon, du moment qu'ils sont accessibles par FTP ou Samba. Vous devrez ensuite transférer le tout sur votre appareil Apple.

GMT Subtitles : **http://goo.gl/VjtIhz**
SubtitlesFinder : **http://goo.gl/rVbrYi**

AVEC UN MEDIA CENTER

Vous avez un Media Center ou un appareil qui fonctionne avec Kodi (ancien nom de XBMC, voir page 41) ? Bien sûr, les sous-titres sont de la partie ! Il faudra néanmoins activer cette fonctionnalité. Allez dans **Système**>**Extension**>**Télécharger des extensions**. Choisissez ensuite **Kodi Add-ons** puis **Sous-titres** et enfin **Opensubtitles.org**. Installez l'extension et activez-la dans **Personnaliser**>**Réglages de l'OSD Vidéo**>**Extension Sous-titres**. Notez que ces chemins peuvent changer si vous avez choisi un autre thème que celui par défaut. Réglez la langue principale sur **Français**. Lancez une vidéo et regardez les sous-titres proposés en cliquant sur le bouton en bas à droite de votre lecteur.

PAS À PAS

Les sous-titres, c'est automatique !

CE QU'IL VOUS FAUT

VLSUB

OÙ LE TROUVER ? :
https://github.com/exebetche/vlsub

DIFFICULTÉ :

01 RÉCUPÉRATION DU FICHIER LUA

Le même fichier LUA vous servira, quel que soit votre système d'exploitation (Windows, Mac, Linux). Sur la page du projet, faites un clic droit dans **vlsub.lua** puis **Enregistrer la cible du lien sous...** avec Firefox ou **Enregistrer le lien sous avec Chrome**. Il faudra ensuite mettre le fichier dans un répertoire **extensions** que vous aurez créé pour l'occasion (si vous n'avez jamais utilisé ce type de fichiers). Ce dossier ira dans **ProgramFiles(x86)\VideoLAN\VLC\lua**.



02 L'INTERFACE

Redémarrez éventuellement VLC et après avoir lancé une vidéo, allez dans le menu **Vue** et cliquez sur **VLSub 0.9.9** pour faire apparaître l'interface. Choisissez la langue des sous-titres et cliquez sur **Search by name** pour trouver un sous-titre correspondant au nom. **Search by hash** permet de trouver un sous-titre correspondant directement à l'empreinte numérique de votre film même s'il est nommé n'importe comment. Si vous avez des difficultés ou si l'extension ne fonctionne pas sous Windows7 & 8, il faudra utiliser l'installeur: **http://goo.gl/SXQrDl.**



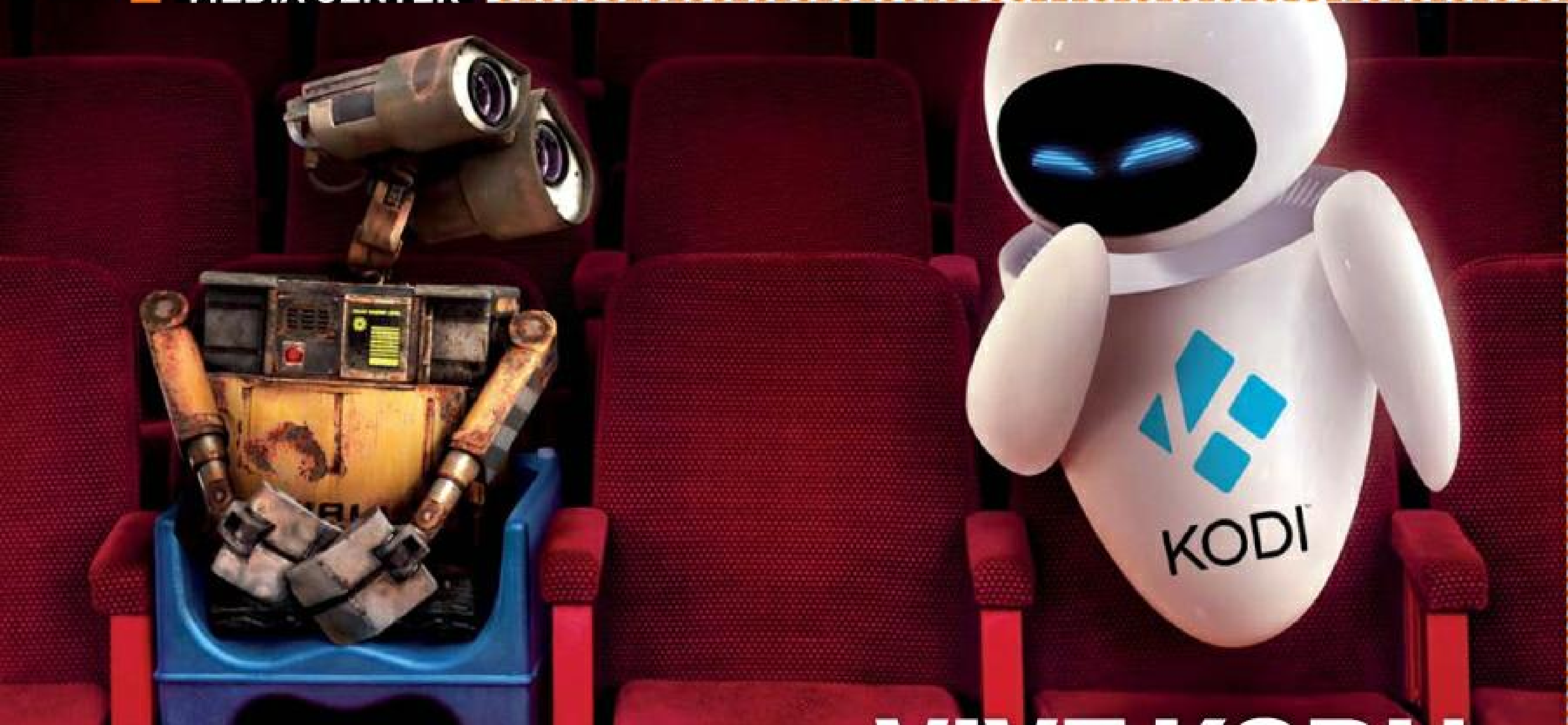
02 LE RÉSULTAT

Sélectionnez le sous-titre dans la liste et cliquez sur **Download selection**. Le sous-titre devrait s'afficher immédiatement dans votre fenêtre. Si ce dernier ne correspond pas à ce que vous recherchez, trouvez-en un autre ou si vous constatez un décalage entre la parole et les textes, vous pouvez corriger cela avec les touches **G** et **H** du clavier (retarder et avancer l'apparition des sous-titres).





NOS GUIDES WINDOWS
100% PRATIQUES
POUR UN PC
+ Puissant
+ Beau
+ Pratique
+ Sûr
Mini Prix : 3€
SEULEMENT 3€ N°16 Janv. / Mars 2015
WINDOWS PC
TRUCS & ASTUCES
BEST OF FICHES PRATIQUES
LE GUIDE COMPLET WINDOWS 8
UTILISEZ FACILEMENT WINDOWS 8
Toutes les astuces
Guide d'achat TEST DE LA Surface Pro 3 + PC Portables & Tablettes !
Personnalisez l'interface
Dopez les performances
TOUT FAIRE : Office, Cloud, Applis, Multimédia, Sécurité, Jeux, etc!
Des dizaines de FICHES PRATIQUES et de LOGICIELS GRATUITS
Passer à WINDOWS 10
Quand, Comment ? Quelles nouveautés ?
Chez votre marchand
de journaux



XBMC EST MORT, VIVE KODI !

Le logiciel Media Center XBMC change de nom pour devenir Kodi. Le concept ne change pas d'un iota, mais les nouveautés sont suffisamment intéressantes pour refaire le point sur ce projet. Voyons comment mettre en place et utiliser ce Media Center sur PC puis examinons ses différentes versions...

XBMC a commencé sa carrière en 2002 où il faisait office de Media Centre sur les premières Xbox modifiées. Le logiciel a fait du chemin puisqu'il a successivement séduit les utilisateurs de Windows, Linux, Android, Mac OS et dorénavant iOS (voir à la fin de l'article). À chaque fois la recette est la même : le but est de réunir tous vos fichiers multimédias sur une même interface pour les retrouver facilement et ne pas avoir à lancer un logiciel pour vos MP3, un autre pour vos films, un autre pour télécharger, etc. Une fois installé sur votre PC, il faudra passer quelques minutes à le paramétrer pour lui dire où aller chercher tel ou tel fichier, choisir son thème, trouver l'accès aux autres machines, etc. La prise en charge du réseau est d'ailleurs un gros plus puisque vous pouvez très bien «aller chercher» vos photos, musiques et films sur un autre PC faisant office de serveur, un NAS ou même un appareil mobile. Les protocoles compatibles sont légions (UPnP, SMB, NFS, etc.) et l'interface n'a rien de bien compliquée. Notons que l'interface est très bien pensée que vous utilisiez une télécommande, un écran tactile, un clavier ou une télécommande compatible.

UNE INTERFACE PERSONNALISABLE

Kodi se révèle très impressionnant dans votre salon. En effet, si vous avez un vieil ordinateur, il est très facile de se confectionner un Media Center digne de ce nom puisqu'il est même possible d'ajouter une télécommande. Le logiciel supporte presque tous les formats et extensions de fichiers multimédias même les plus récents. Il intègre en plus des fonctionnalités comme la compatibilité avec les formats les plus courants de playlist, des diaporamas, la possibilité de streamer ou d'écouter des radios Internet comme SHOUTcast et Last.fm. La communauté est tellement vivace que de nombreux plugins sont développés pour permettre d'enrichir votre interface. Il est, par exemple, possible d'avoir des bulletins météo, de lire vos flux RSS, de récupérer des sous-titres directement depuis l'interface ou d'avoir accès à l'Internet Movie Database et CDDB pour récupérer des informations sur vos albums ou vos films. Il est même possible de télécharger en utilisant Torrent, de regarder ses mails ou d'avoir accès à sa page Facebook. Si vous utilisez votre PC pour vos loisirs numériques, vous allez vite délaisser Windows pour ne jamais sortir de ce Media Center !

QUOI DE NEUF AVEC KODI ?

En plus de la compatibilité avec les appareils iOS jailbreakés (avec support de Airplay), Kodi 14 prend en charge les derniers codecs compatibles 4K : VP9 et H.265. Pour en profiter, il faudra bien sûr un appareil puissant ainsi qu'un écran compatible avec cette nouvelle norme 4 fois plus détaillée que le Full HD actuel.

LEXIQUE

***MEDIA CENTER :** Media Center peut désigner un disque dur multimédia relié à une TV ou un Home Cinema mais nous ne parlerons ici que de la partie logicielle. Kodi est un programme qui peut se greffer sur presque n'importe quel système pour en faire une interface de lecture conviviale

PAS À PAS

Premier pas avec Kodi

CE QU'IL VOUS FAUT

KODI 14 (HELIX)

OÙ LE TROUVER ? :
http://kodi.tv

DIFFICULTÉ :

01 L'INSTALLATION

Après avoir installé le logiciel, votre pare-feu va sans doute vous demander l'autorisation de faire communiquer Kodi avec Internet.



Dites **Oui** surtout, si vous utilisez le réseau local pour faire transiter vos fichiers. Il faudra ensuite changer la langue par défaut si vous êtes allergique à l'anglais. Depuis la fenêtre principale, allez dans **System** (tout à droite) puis **Settings**. Dans l'onglet **Apparence,** cherchez le **français** dans **Langue** et **Région**. Changez aussi l'agencement du clavier.

02 VOTRE THÈME

Vous pouvez ensuite aller dans **Thème** et cliquer sur **Plus...** pour



télécharger d'autres habillages. À vous de trouver celui qui vous conviendra le mieux, mais sachez que certains thèmes proposent davantage d'entrées au menu principal comme **Concert**, **Météo**, **Série TV**, etc.

03 TROUVEZ VOS FICHIERS

Pour commencer l'aventure, il va falloir dire au logiciel dans quel(s) dossier(s) aller chercher vos différents répertoires multimédias. Par exemple dans **Musique**, cliquez sur **Fichiers** puis **Ajouter une source**. Ici, il faudra chercher dans votre disque dur le ou les dossiers où vous avez l'habitude de ranger vos MP3. Si vous avez



plusieurs genres de musique, rien ne vous empêche de les organiser dans Windows ou depuis Kodi. Dorénavant, lorsque vous irez dans **Musique>Fichiers**, vous aurez tous vos albums et morceaux dans une liste!

04 LES OPTIONS

Faites de même dans les autres catégories **Images** et **Vidéos**. Le procédé est le même que pour **Musique**. Notez qu'à chaque fois vous avez la possibilité de mettre plusieurs dossiers. Pour les photos, vous aurez une prévisualisation des fichiers sur le côté droit et il suffit de



passer la souris sur le panneau déroulant à gauche pour lancer un diaporama, trier ou filtrer vos fichiers par date, taille, etc. Pour les albums, vous aurez accès automatiquement à la pochette si elle est disponible. Pour les films, il faudra avoir recours à une extension.

05 AJOUTER DES EXTENSIONS

Pour ajouter une extension (le nom que donne le logiciel aux différents plugins, les programmes complémentaires), il suffit de cliquer dans **Système>Extensions** puis de choisir la rubrique de votre choix. Vous pouvez même rechercher par mots clés. Vous pouvez par exemple ajouter une version de µTorrent, de Dropbox, un tchat IRC, l'application Facebook et bien sûr des plugins pour afficher une mine d'informations pour vos films et séries TV.



UN MEDIA CENTER MULTISUPPORT

Outre votre bon vieux PC sous Windows, Kodi est disponible sur plusieurs plates-formes. Parfois il vient se greffer sur un système existant et parfois il fait aussi office de système à part entière. Vous avez forcément un appareil concerné par Kodi !

LINUX

Kodi (anciennement Xbox Media Center) était à l'origine un logiciel codé pour la version non signée de Linux sur la première Xbox. Pas étonnant donc de voir que le programme se plaît très bien sur cet OS, quelle que soit la distribution. Il existe même une version «standalone» appelée Kodibuntu qui permet de se confectionner un Media Center sur un PC vieillissant sans avoir à installer de système complexe et gourmand en ressource.



MAC, IOS ET APPLETV

Kodi est compatible avec les Mac sous réserve d'avoir au moins Mac OS X 10.6. L'Apple TV 2 est aussi de la partie. Pour les appareils sous iOS, il vous faudra bien sûr un matériel jailbreaké. Installez IFile depuis Cydia puis téléchargez Kodi. Vous trouverez les procédures en suivant les Wiki de ce lien : **http://kodi.tv/download.**



RASPBERRY PI

N'oublions pas le Raspberry Pi ! Ce nano-ordinateur a plus d'un tour dans son sac et propose pas moins de trois distributions prêtes à l'emploi pour installer Kodi : Raspbmc, Xbian et OpenELEC que nous avons déjà abordé dans notre numéro 18. Si la mise en place d'un Media Center sur Rasberry Pi vous intéresse, retrouvez sur notre CD le PDF de l'article à ce sujet. Pour plus de détail : **http://kodi.wiki/view/Raspberry_Pi.**



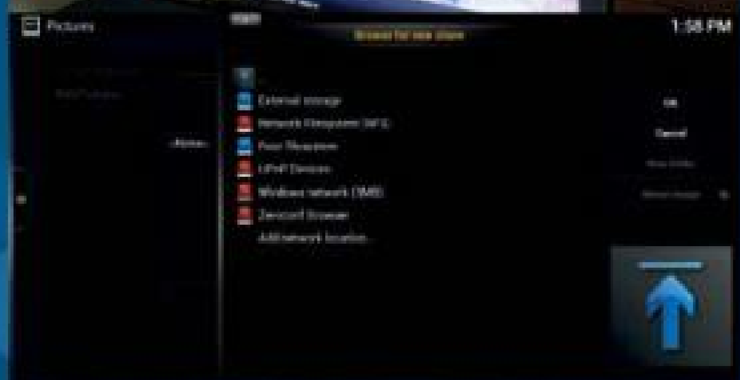


ANDROID

Kodi dispose aussi de versions Android pour processeur ARM ou x86. Sur appareil mobile, Kodi est léger et répond au doigt et à l'œil. Récupérer vos fichiers dans un réseau local est un jeu d'enfant et rares sont les formats qui ne sont pas pris en compte. Pour pousser le test un peu plus loin nous avons même pu installer Kodi sur l'Android Media Player CVJI-E212 que nous avons testé dans le numéro 17. Bien que possédant déjà un logiciel de lecture, Kodi a remplacé avantageusement ce dernier et s'est même payé le luxe d'être compatible avec la télécommande fournie !









TÉLÉCHARGEMENT DIRECT : LE GUIDE 2015



Moins compliqué à comprendre que BitTorrent, moins contraignant (inscription à un tracker, respect du ratio, etc.) et moins dangereux, le téléchargement direct est toujours l'une des solutions préférées des Français. Voyons quels sont les forces en présence, les nouveautés et tous ses petits secrets...

LEXIQUE

***DDL :**
Abréviation de «Direct DownLoad». Il s'agit de téléchargement dit «direct» car il ne passe pas un protocole P2P ou décentralisé. Ici, comme au bon vieux temps, le fichier convoité est sur un serveur et vous le rapatriez sur votre disque dur en utilisant le protocole «classique» d'Internet (HTTP).

Le monde du téléchargement direct (DDL) change plus vite que celui du P2P. Ce denier est largement décentralisé ce qui empêche la moindre action des ayants droit : pas facile de faire interdire un logiciel ou un protocole. Au contraire, le côté centralisé du DDL (des fichiers stockés sur des serveurs) oblige les acteurs à changer... ou à mourir comme MegaUpload. La méthode ne change pas, mais l'emplacement des fichiers oui. Et même si les syndicats font souvent le ménage et intentent des procès à ceux qui voudraient prendre le chemin de MegaUpload, il est difficile d'endiguer cette méthode de téléchargement. À l'inverse du P2P où les aficionados sont traqués par HADOPI, les téléchargeurs sont tranquilles avec le DDL (le protocole «standard» HTTP utilisé ici passe inaperçu) alors que ce sont les plates-formes qui sont la cible des ayants droit. Mais comment cela fonctionne-t-il ?

COMMENT ÇA MARCHE ?

Le téléchargement direct s'organise comme ceci. Il faudra, en premier lieu, trouver un point d'entrée pour trouver les liens vers les fichiers. Ce point d'entrée est généralement un site de référencement, un blog ou un forum. Certains demanderont de vous abonner et d'autres non. Leur point commun est de répertorier et trier des liens qui redirigent vers des fichiers multimédias. Auparavant, 80 % des fichiers de téléchargement direct étaient hébergés sur feu MegaUpload. Mais ces derniers sont désormais stockés ailleurs, répartis sur les serveurs de nombreux hébergeurs : FileFactory, Uploaded, RapidGator, BitShare et des dizaines d'autres. Mais la guerre continue : Hotfile a, par exemple, subi les foudres de la MPAA l'année dernière...



Sur les sites de DDL, on trouve beaucoup de contenus... mais aussi beaucoup de publicités !

LES LIMITES DE LA GRATUITÉ

Cette multiplication des hébergeurs permet aussi aux uploaders de ne pas mettre leurs œufs dans le même panier. On constate en effet que les contributeurs sont présents sur plusieurs hébergeurs. Le problème avec ces derniers c'est qu'ils ne vivent pas d'amour et d'eau fraîche. Des serveurs, ça se paye et ils sont prêts à tout pour vous faire sortir le portefeuille. Les limitations des utilisateurs gratuits sont en effet nombreuses et dépendent des hébergeurs. Souvent, la taille des fichiers sera limitée à 1 ou 1,4 Go et il ne vous sera pas possible de faire plus d'un téléchargement en même temps. Vous devrez aussi attendre tant de secondes avant de pouvoir cliquer sur le lien permettant de télécharger et vous n'aurez pas accès aux «hotlinks». Ces liens dirigent directement vers le fichier convoité, sans captcha (ces dispositifs qui vérifient que vous n'êtes pas un «robot»), et permettent de placer directement le lien dans un logiciel de téléchargement pour ne pas les gérer dans votre navigateur. Il s'agit de divers stratagèmes destinés à inciter les utilisateurs à s'inscrire ou à payer.

DES LOGICIELS INTELLIGENTS

Mais certains logiciels comme JDownloader ou MiPony permettent de déjouer ces méthodes. Bien sûr, vous resterez un utilisateur gratuit avec toutes les limitations, mais vous n'aurez pas besoin de cliquer 5 fois sur telle page, subir la dizaine de publicités pour, au final, avoir enfin le lien convoité. Ces logiciels feront le travail à votre place. Il vous suffira de coller l'URL de la page contenant les liens et ils se chargeront de récupérer le fichier directement, comme si vous aviez un «hotlink». MiPony propose même des plug-ins permettant de déjouer les captchas. Plus besoin de déchiffrer ces horribles mots tordus...

LE DDL, LA BONNE SOLUTION POUR VOUS ?

Attention, comme nous venons de le voir, même avec un logiciel de ce type, vous n'aurez pas les avantages du «Premium». Le plus frustrant, c'est le débit descendant ridicule. Un film pourra mettre 4 ou 5 heures à arriver en intégralité sur votre disque dur (entre 50 et 100 kb/s) même si certains hébergeurs peuvent proposer plus à certains moments de la journée (350 kb/s sur UptoBox par exemple). Rien de bien insurmontable, si vous voulez regarder un film le soir, mais les possesseurs de la fibre accros aux P2P auront bien du mal à ne pas s'arracher les cheveux. Le DDL gratuit est donc la solution idéale pour les téléchargeurs occasionnels. Les fondus du téléchargement opteront pour le P2P (avec VPN) ou pour un mode payant chez un hébergeur ou un débrideur (voir notre encadré).

Pour vous vendre leur solution, les hébergeurs vous aguichent avec des vitesses très élevées... en Premium uniquement !



PAS À PAS

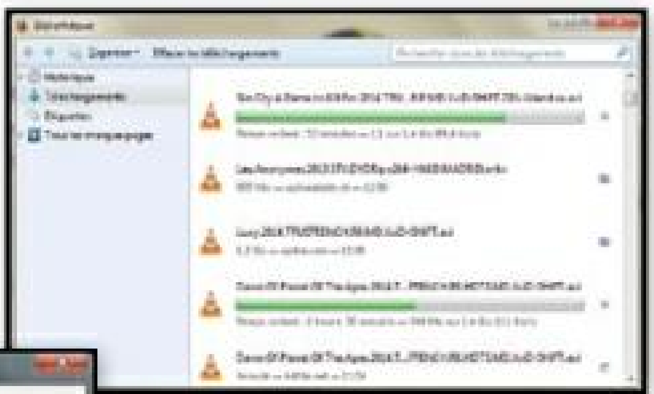
Télécharger sans logiciel

01 TROUVER UN LIEN

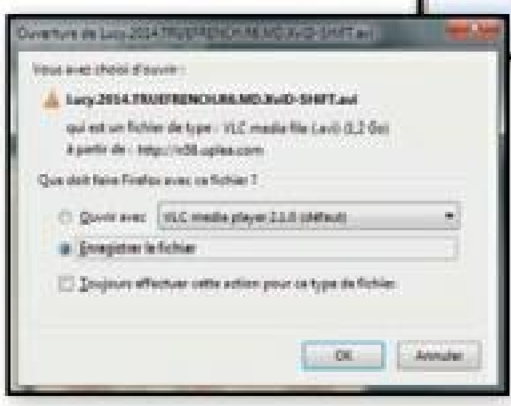


Commençons par un site de notre liste comme eMule-Island et choisissons un fichier dans la liste. Sur ce site, cliquez ensuite sur **Direct Download** pour avoir la liste des liens. Après, il faudra choisir en fonction de l'hébergeur. Parfois, il faudra absolument vous inscrire et parfois, vous n'aurez qu'à taper un captcha. Dans tous les cas, le téléchargement sera bridé.

02 LA VALSE DES HÉBERGEURS



Au bout de quelques jours, vous trouverez ceux qui sont les plus rapides ou ceux qui affichent le moins de pub. Pour la plupart, vous devrez attendre quelques secondes avant de pouvoir cliquer. Normalement, le navigateur prend la relève à ce moment et vous n'aurez qu'à valider pour commencer le téléchargement comme n'importe quel autre fichier.



03 LES LIMITATIONS

L'interface de MiPony n'a rien de sorcier. Sur une page Mais il existe des limitations, surtout quand on refuse de payer. Sur certains hébergeurs, vous n'aurez accès au fichier qu'à condition de payer, ailleurs, il faudra se contenter de fichier pesant moins de 1 Go ou d'une limitation du nombre de téléchargements, etc. Bien sûr, rien ne vous empêche de télécharger 10 fichiers sur 10 hébergeurs différents en passant par le même site de référencement !



TOP 3 DES SITES DE TÉLÉCHAR

> eMule-island



Une destination de choix pour trouver films, séries, documentaires et animés. Il a le mérite de comporter des liens de téléchargement direct, mais aussi de stream et de Torrent. Le site est très bien conçu avec peu de publicités, différentes catégories (HD, Top 20, etc.) et même des tutos pour aider un peu les débutants. Le seul problème c'est que les logiciels de téléchargement ne détecteront pas les liens concentrés sur une seule et même page. Il faudra les copier-coller un à un. Rien d'insurmontable d'autant que les liens morts sont peu nombreux.

Lien : **www.emule-island.ru**

LE SAVIEZ-VOUS ?

Même si les sites qui proposent des liens n'hébergent rien sur leurs serveurs, ils peuvent être accusés de favoriser et d'inciter au piratage de biens culturels. Ainsi rares sont ceux qui ne sont pas hébergés eux-mêmes dans un pays «exotique». Vous voyez beaucoup d'URL qui se termine par .cc, .tv, .ws ou .ru ? C'est normal, les nouveaux eldorados du téléchargement direct sont aux îles Coco, au Tuvalu, aux Samoa occidentales ou en Russie...

0110101010001001101010001000101010110010010010101000 10 0101001010010101010100 10000

Télécharger avec MiPony

CE QU'IL VOUS FAUT

MIPONY

OÙ LE TROUVER ? : **www.mipony.net**

DIFFICULTÉ :

01 AVEC MIPONY



Si télécharger «à la main» ne vous satisfait pas, MiPony va vous faciliter la tâche. Il va scanner une page Internet comprenant tous les liens d'un même film puis les analyser pour y accéder directement. Il faudra taper le captcha à la main, mais c'est un moindre mal. Sachez cependant qu'un plug-in MiPony additionnel règle ce problème.

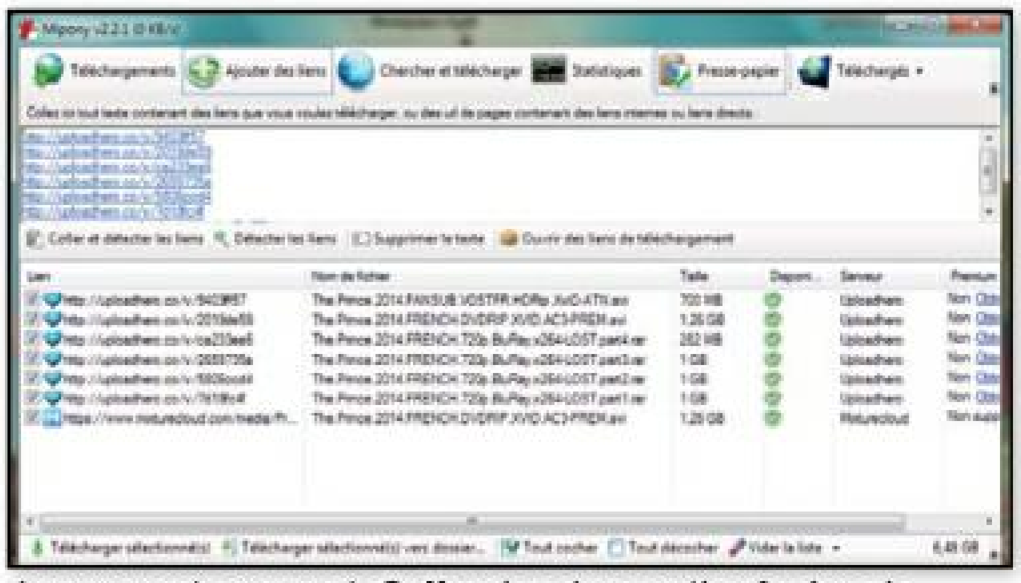
02 ATTENTION NUISIBLE !



Attention lors de son installation, il faudra être prudent, car MiPony - à l'instar de son concurrent JDownloader - vous proposera l'installation de plusieurs logiciels nuisibles: toolbars, scan du registre, etc. À vous de décliner les offres ou de décocher les cases (**Custom Installation**) pour éviter ces «poubellewares»...

03 L'ANALYSE DES LIENS

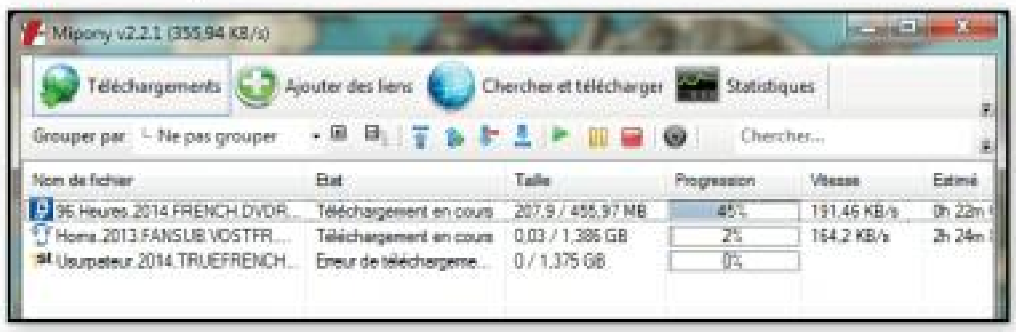
L'interface de MiPony n'a rien de sorcier. Sur une page comprenant plusieurs liens, faites **Copier** dans la barre d'adresse



de votre navigateur puis **Coller** dans la première fenêtre de l'onglet **Ajouter des liens**. Cliquez ensuite sur **Détecter les liens**. Normalement dans la fenêtre du bas, les différents liens actifs vont s'afficher avec les icônes correspondantes à leurs hébergeurs respectifs.

04 LE TÉLÉCHARGEMENT

En faisant un simple clic droit puis **Télécharger**, vous enverrez les liens dans l'onglet **Téléchargements** où ils commenceront leur progression. Si, dès l'onglet **Ajouter des liens**, MiPony ne détecte rien, il faudra essayer les liens un à un. Heureusement dans notre liste, rares sont les sites qui ne seront pas «compatibles» et, dans le cas contraire, les liens morts sont souvent effacés.



GEMENT DIRECT

> WawaCity



Un très bon site qui enregistre automatiquement des liens dans le presse-papiers pour JDownloader ou MiPony. Pour utiliser cette fonctionnalité, il suffit de cocher les cases correspondantes aux fichiers et de cliquer sur le bouton adéquat. Votre gestionnaire de téléchargement ira directement chercher les liens pour télécharger le plus rapidement possible. WawaCity propose des vidéos, des séries, des eBooks, des animés et même des jeux et des logiciels !

Lien : **www.wawacity.su**

> LibertyLand



Un autre très bon site où vous pourrez choisir entre VF et VOSTFR pour les vidéos. Vous trouverez aussi des liens pour le stream et le téléchargement BitTorrent. Les utilisateurs Premium ou utilisant un débrideur ont aussi leur propre catégorie pour obtenir des «hotlinks».

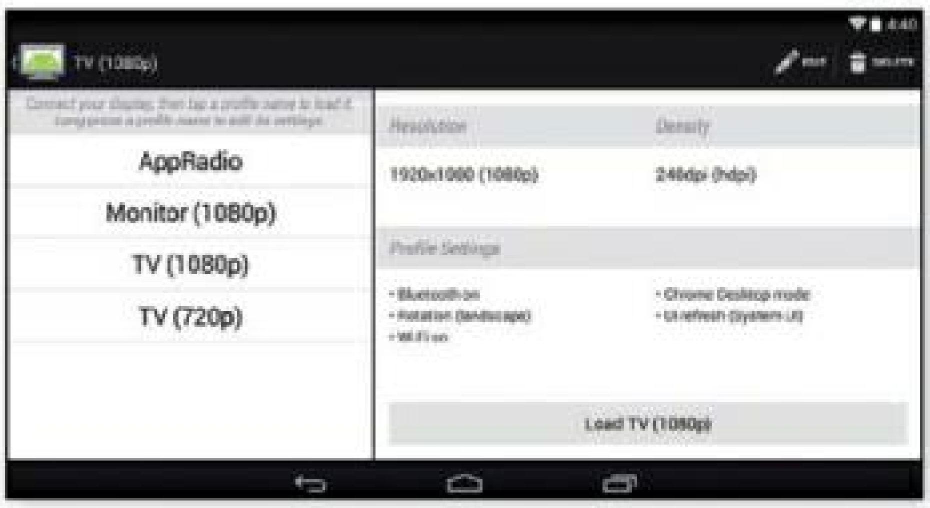
Lien : **www.libertyland.tv**

#1 Adapter la résolution

AVEC SECONDSCREEN

SecondScreen va vous changer la vie si vous avez l'habitude d'utiliser un autre moniteur pour afficher les photos ou vidéos que vous avez sur votre appareil mobile sous Android. L'appli adaptera la résolution pour avoir la meilleure expérience possible sur votre téléviseur que vous utilisiez Chromecast, un autre système de partage de flux ou simplement votre câble HDMI. Transformez votre appareil Android en console de jeux, PC de remplacement ou disque dur multimédia ! Attention, il vous faudra un appareil rooté.

Lien : **http://goo.gl/wDrKe7**

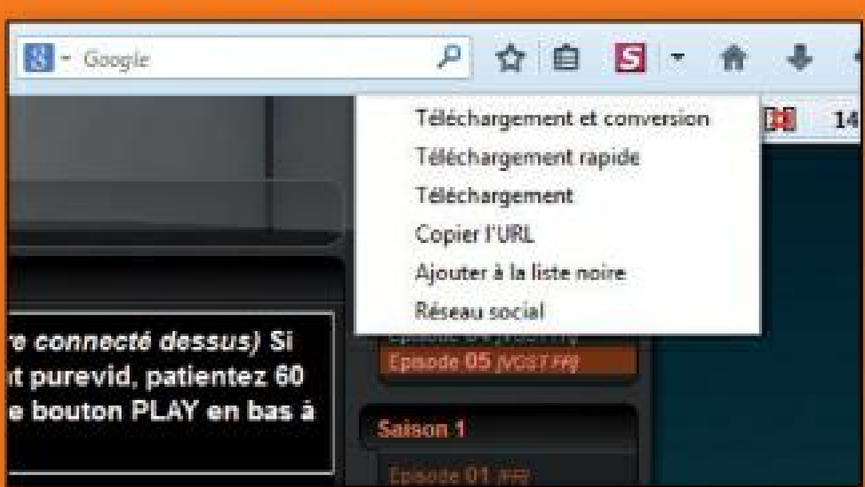


#2 Télécharger du stream

AVEC DOWNLOADHELPER

Vous aimeriez garder une trace de la vidéo qui s'affiche sur votre navigateur ? Qu'il s'agisse d'une plateforme comme YouTube et Dailymotion ou d'un film issu d'un hébergeur multimédia, l'extension DownloadHelper de Firefox va vous sauver la vie. Dès que l'extension va détecter une vidéo que vous pouvez télécharger, l'icône s'anime et une petite flèche apparaîtra sur sa droite. Il suffit alors de cliquer dessus pour choisir sa vidéo. Le secret ? DownloadHelper analyse le code source de la page Web pour en retirer les liens vers les fichiers. Libre à vous ensuite de les télécharger d'un seul clic. Cerise sur le gâteau, DownloadHelper permet sous certaines conditions de convertir la vidéo (la plupart du temps en FLV) vers un format plus souple (WMV, AVI, etc.) ou directement optimisé pour un appareil (Galaxy Tab, iPhone, etc.)

Lien : **http://goo.gl/dJ7B9f**



#3 Enregistrer les chansons de YouTube

AVEC PEGGO

Il existe beaucoup de service permettant d'enregistrer un MP3 depuis une vidéo YouTube mais peu d'entre eux disposent d'options comme la possibilité de spécifier un intervalle, couper les blancs ou normaliser le son. C'est ce que propose Peggo.co. Il suffit de copier-coller l'URL de votre vidéo et faire Record MP3 après avoir réglé vos paramètres depuis l'interface Web. Bien sûr, vous pouvez aussi enregistrer la vidéo en même temps ou garder une trace sonore d'autres émissions, podcasts, etc.

Lien : **http://peggo.co**



#4 Partager votre carte SD via Wi-Fi

AVEC SAMBA FILESHARING

Samba Filesharing est une appli très utile si vous désirez partager le contenu de la carte SD d'un de vos appareil Android sur votre réseau domestique.
Une fois installée sur votre smartphone ou tablette, il suffira de retrouver le contenu de votre carte SD avec votre explorateur Windows comme si la mémoire était une clé USB. Il est même possible de spécifier un mot de passe pour plus de sécurité. Attention, il vous faudra un appareil rooté.

Lien : **http://goo.gl/2cbHgp**



#5 Un Popcorn Time «manga»

AVEC WAIFU

Depuis que le code source de Popcorn Time s'est retrouvé dans la nature, on compte de plus en plus de clones sans saveur du «Netflix des pirates». Pourtant, certains tentent de trouver des thèmes originaux comme Waifu, un logiciel qui ne propose que des animés ! Apparemment, toutes les vidéos sont en espagnol, mais il s'agit d'un bug dans l'interface : vous pouvez très bien choisir la version originale sous-titrée en anglais (et parfois en français) dès que vous avez lancé votre flux vidéo. Certains épisodes manquent de «seed», mais le résultat est plutôt sympa. Les fans de manga se doivent de l'essayer...

Lien : **http://waifu.ca**



#6 Des chaînes du monde entier

AVEC FILMONTV

Fonctionnant sans restriction géographique, le site FilmOnTV propose des centaines de chaîne de télé du monde entier. On y retrouve des canaux français comme Euronews, Arte, iTele, France3, France5 ou BFM TV ainsi que des chaînes russes, italiennes, canadiennes, allemandes ou grecques. Si vous ne savez pas par où commencer, les programmes sont aussi classés par type. Si vous voulez regarder du sport, un film d'horreur, des émissions sur les jeux vidéo ou destinées à la jeunesse, vous n'aurez qu'à cliquer. La HD est disponible gratuitement pour bon nombre de chaînes, mais pour l'enregistrement en HD, il faudra passer à la caisse. Une section pour les appareils mobiles est aussi de la partie.



Lien : **www.filmon.com**

#7 Encoder votre musique en haute qualité

avec FOOBAR2000

les mélomanes qui veulent garder le son de qualité CD, il existe le FLAC, un format «lossless»... Commencez par installer Foobar2000 dans sa version standard puis le codec FLAC. Placez votre CD dans le lecteur et sur le logiciel, allez dans **File>Open audio CD**. Choisissez la lettre du lecteur et faites **Rip**. Le logiciel ira chercher les informations concernant votre album dans une base de données. Faites ensuite **Proceed to the Converter Setup dialog**. Dans cette nouvelle fenêtre, vous devrez cliquer dans **Output format** et choisir **FLAC**. Vous pourrez ensuite aller dans **Edit** pour régler le **Compression Level**. Validez, faites **Back** et **Convert**. Le logiciel vous demandera de pointer vers le codec **flac.exe** que vous avez installé (pas le fichier d'installation, mais le EXE contenu dans **C:\Program Files (x86)\FLAC)**. Et c'est parti pour la conversion !

Lien : **www.foobar2000.org**

Lien : **https://xiph.org/flac**





X-MATÉRIELS

> ELM327 Car Diagnostics OBDII



Le câble de diagnostic ELM327 est un microcontrôleur qui relie votre PC (ou un appareil mobile Android) à votre voiture en utilisant l'interface OBDII. Cette dernière équipe toutes les voitures depuis le début des années 2000. L'appareil est livré avec un CD de 8 cm comportant les drivers, les différentes applis pour Android et trois logiciels Windows permettant de traiter et d'analyser les différentes informations collectées : la température du liquide de refroidissement, l'état du système de carburant du véhicule et d'autres données concernant la vitesse et la puissance. Il est même possible d'effacer des voyants d'alerte et de monitorer certains paramètres moteurs. Un outil sympa que nous avons choisi de vous présenter en détail...

Prix : **20 €** **www.chinavasion.com**

> Novodio Multi Fast Charger,

UN CHARGEUR RAPIDE, INTERNATIONAL ET POLYVALENT



Avec tous nos appareils mobiles, faire sa valise devient un vrai casse-tête lorsqu'il s'agit de savoir quel chargeur emporter pour quel matériel. Le Novodio Multi Fast Charger propose une solution astucieuse. Non seulement l'appareil permet de recharger 4 machines en même temps, mais elle propose deux intensités (2x 1A et 2x 2,4A) pour répondre aux différents besoins en énergie. Rien ne vous empêche d'ailleurs de recharger un smartphone nécessitant 1A sur une prise 2,4A . Comme la tension reste au alentour des 5V, votre batterie de risque rien et vous diviserez par deux votre temps de recharge. Cerise sur le gâteau, la prise secteur est interchangeable et 3 autres types de broches sont fournis : Royaume-Uni, USA et Australie (les pays d'Asie ou d'Afrique utilisent forcement un de ces 4 standards).

Prix : **40 €** **www.novodio.com**



> Creator CI20,

UN NOUVEAU CHALLENGER POUR LE RASPBERRY PI

Les nano-ordinateurs ont le vent en poupe ! Après le Raspberry Pi, le Gizmo 2, les différents BeagleBone ou la gamme HummingBoard, voici le Creator CI20. Et le moins qu'on puisse dire c'est que les caractéristiques techniques mettent une petite claque au projet de David Braben : processeur de 1.2 GHz à double cœur, 1 Go de DDR3, 2 ports USB dont un «host» (USB OTG) ainsi que du WiFi et 8 Go de mémoire de stockage en natif. Le chipset vidéo est aussi plus avancé et permet d'afficher en hard du H.264, du VP8 ou du RV9. On imagine très bien le Creator CI20 faire office de Media Center HD, de PC d'appoint ou d'être utilisé dans un projet «jeu vidéo» : console multisupport ou borne d'arcade. Il faudra bien sûr attendre que la communauté s'étoffe et propose des distributions adaptées et optimisées...

Prix : **50 €**
www.imgtec.com

ELM327, un outil de diagnostic auto bon marché!

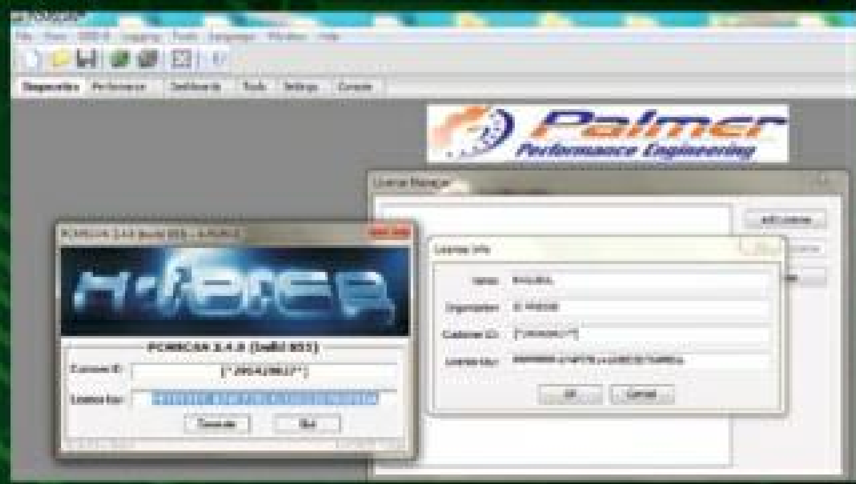
Voyons comment un appareil à 16 € (21 € avec les frais de port) peut vous renseigner sur l'état de voiture et sur ses performances...



#1 DANS LA «BOÎTE»

Pas de fioriture au niveau de l'emballage puisque nous avons reçu l'ELM327 et son CD d'installation dans une pochette en plastique. Dans un premier temps, il faudra installer les pilotes CP2102 sous Windows à moins que vous ne souhaitiez utiliser un appareil Android pour monitorer votre auto. Dans ce cas il faudra installer les fichiers APK et s'assurer que votre matériel dispose d'une prise USB OTG (un port USB Host permettant le branchement d'un connecteur de type A). Sachez aussi que des périphériques OBDII compatibles Bluetooth sont disponibles sur le marché.

#2 LES LOGICIELS



Sous Windows, le CD contient les logiciels PCM Scan, ScanTool.net et ScanMaster. Le premier ne dispose pas d'interface en français tandis que le second est un peu rudimentaire. Nous avons donc utilisé le dernier avant tout, mais rien ne vous empêche de tous les essayer. Ces programmes sont normalement payants, mais ici notre fournisseur chinois a eu la gentillesse de nous fournir les keygen pour faire fonctionner le tout ! Lorsque vous vous demandera d'enregistrer le produit avec un code utilisez ces générateurs de clés.

#3 OÙ EST LE PORT OBDII ?

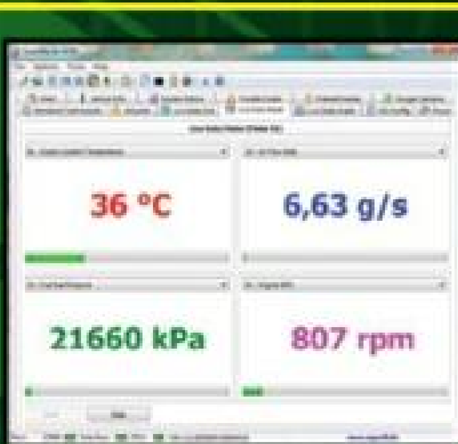


Il faudra ensuite trouver le port OBDII sur votre véhicule en vous aidant de la notice. Chez nous il est au fond de la boîte à gants. Le site dresse une liste de marque de voiture compatible, mais elle reste assez vague. Par exemple sur notre Dacia Sandero de test, le produit a fonctionné sans problème alors que la marque n'est pas dans la liste. Notez aussi que certaines fonctions ne seront pas disponibles avec tous les types de véhicules. Reliez le PC à la voiture et mettez le contact (le moteur n'a pas forcement besoin de tourner pour la connexion, mais il faut que le tableau de bord soit allumé).



#4 LA CONNEXION

Sur ScanMaster, à l'onglet **Start** faites **Connect** (allez dans les **Options** pour l'interface en français) et attendez le message **ECU Connected**. Dans **System Status** regardez avec quelle option votre véhicule est compatible. Dans **Live Data Meter** et **Live Data Graph** vous pourrez choisir d'afficher différentes données en temps réel: température du liquide de refroidissement, débit d'air, régime moteur, pression de la rampe d'injection et une vingtaine d'autres données. Bien sûr toutes ces informations peuvent être enregistrées.



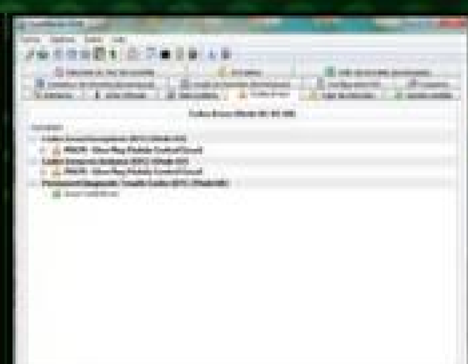


#5 ALLONS PLUS LOIN...

Notez que certaines de ces données ne pourront être calculées qu'avec le moteur en marche et d'autres avec le véhicule en mouvement (pour tout ce qui concerne la vitesse, la consommation, etc.) Dans l'onglet **Power** vous pourrez avoir encore plus d'indications sur les performances de votre voiture à condition de remplir un petit formulaire: poids du véhicule, nombre de rapports, type de pneu, etc. Vous pourrez ainsi obtenir des données concernant l'accélération, les rapports **puissance/couple** et **RMP/vitesse**. Enfin dans **Trouble Codes** vous pourrez effacer des voyants lumineux s'affichant sur votre tableau de bord.







CD OFFERT

LE PACKAGE DU PIRATE

Tous les logiciels INDISPENSABLES

100% GRATUIT

LE GUIDE PRATIQUE

100% MICRO-FICHES, TRUCS & ASTUCES

SURVEILLANCE

BACKUP

TOR

WEB CACHÉ

MiPony

PROTECTION

SMARTPHONE

Bons plans

Réseaux

EFFACER

DÉMASQUER

NSA

TÉLÉCHARGER

BEL : 6 € - DOM : 6,10 € - PORT.CONT. : 6 € - CAN : 7,99 $ cad - POL/S : 750 CFP - TUN : 9,8 tnd

L 12730 - 24 - F: 4,90 € - RD